HRUŠKA & CO.

ADVOKÁTNÍ KANCELÁŘ

ATTORNEYS AT LAW

TÁBORSKÁ 619, 140 00 PRAHA 4
TEL. +420 241 404 199, +420 241 401 128 FAX +420 241 409 142
E-MAIL: hruska@ak.cz

V Praze, dne 25.5.2018

Vážení klienti a přátelé,

zcela jistě Vám na síti internet a z médií neuniklo, že dne 25. 5. 2018 vstupuje v účinnost Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů, **tzv. GDPR**, které ve všech státech EU reguluje ochranu osobních údajů fyzických osob.

Dle mediálních a marketingových zpráv se může zdát, že jde v České republice o naprostou novinku či převratnou revoluci v ochraně osobních údajů, nicméně tento dojem je mylný, neboť v našem státě je již ochrana osobních údajů regulována, a to zákonem č. 101/2000 Sb. ve znění pozdějších předpisů (o ochraně osobních údajů – dále jen ZOOU), který nabyl účinnosti dne 1.6.2000.

Rádi bychom Vás stručně tímto dokumentem informovali o některých základních pojmech, s nimiž GDPR pracuje, a o základních povinnostech, které musí správce popř. zpracovatel k ochraně osobních údajů dle GDPR plnit. A snad se nám strohou právnickou řečí povede vyvrátit i některé mýty šířené ve veřejném prostoru.

Nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Nevztahuje se mj. např. na zpracování údajů prováděných fyzickou osobou v průběhu výlučně osobních či domácích činností.

<u>Některé základní pojmy</u>
Osobní údaj – veškeré informace o identifikované či identifikovatelné fyzické osobě (subjektu údajů); identifikovatelnou fyzickou osobou je pak fyzická osoba, kterou lze přímo nebo nepřímo identifikovat pomocí identifikátoru, jako je například jméno, identifikační číslo, lokační údaje, apod. Zjednodušeně řečeno půjde o údaj či soubor údajů, podle nichž lze určit konkrétní fyzickou osobu (např. jméno, příjmení, datum narození).

Citlivý osobní údaj – údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, dále genetické či biometrické údaje (např. zobrazení obličeje, otisk prstu), údaje o zdravotním stavu, sexuálním životě, sexuální orientaci, ale i o trestních deliktech či pravomocném odsouzení osob. Jde o údaje, které mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Jejich zpracování podléhá mnohem přísnějšímu režimu, než zpracování údajů nikoli citlivých; v zásadě až na zákonné výjimky je lze zpracovávat jen na základě souhlasu subjektu údajů.

Zpracování osobních údajů - jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn buď bez pomoci nebo s pomocí automatizovaných postupů (shromáždění, zaznamenávání, uspořádání, strukturování, uložení nebo pozměnění či vyhledávání, šíření, zpřístupnění, seřazení, kombinování, blokování, výmaz, zničení atd.). Zpracování ve smyslu GDPR je tedy činnost, kterou správce s osobními údaji provádí za

určitým účelem a z určitého pohledu tak činí systematicky (např. shromažďuje a eviduje osobní údaje zákazníků za účelem plnění s nimi uzavřené smlouvy).

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. Zjednodušeně řečeno ten, kdo operace s osobními údaji provádí, buď z vlastního rozhodnutí, nebo proto, že je to jeho zákonnou povinností. Správcem může být i fyzická osoba, pokud zpracovává osobní údaje způsobem, že tento způsob již vylučuje uplatnění výjimky osobní či domácí činnosti, resp. pokud nejde o nakládání s osobními údaji, které ještě nesplňuje definici jejich zpracování.

Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Souhlas subjektu údajů – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

Právní důvody zpracování

Právní důvody zpracování znamenají pro správce oprávnění osobní údaje zpracovávat pro ten který konkrétní účel. Aby tedy správce mohl osobní údaje legálně zpracovávat, musí k tomu mít alespoň jeden z následujících právních důvodů:

a) zpracování je nezbytné pro splnění smlouvy, jejíž stranou je subjekt údajů nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů (např. údaje zákazníka nezbytné pro účely uzavření smlouvy, dodání zboží a vystavení faktury)

b) zpracování je nezbytné pro splnění právní povinnosti, kterou má správce uloženu (např. údaje o zaměstnanci nezbytné pro to, aby zaměstnavatel mohl za něho odvést povinné odvody)

c) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby

d) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,

e) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany krom případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadujících ochranu osobních údajů

f) subjekt údajů udělil souhlas pro jeden či více konkrétních účelů

Zpracování se vždy váže k účelu zpracování; na základě něho se určí právní důvod. U každého zpracování osobních údajů je třeba tedy třeba určit účel a podle něho pak to, zda má správce některý z právních důvodů pro zpracování uvedených výše pod písm. a)-e). Teprve pokud žádný z takových důvodů není dán a přesto chce správce údaje zpracovávat, potřebuje k tomu souhlas subjektu údajů.

Souhlas subjektu údajů

Pokud je tedy zpracování založeno na souhlasu subjektu údajů, musí být správce schopen doložit, že subjekt údajů souhlas udělil. Jak již výše uvedeno, souhlas musí být svobodný,

konkrétní, informovaný a jednoznačný. Jde o aktivní a dobrovolný projev vůle, k němuž subjekt údajů nemůže být (ani nepřímo) nucen. Žádost o souhlas musí být jednoznačná, srozumitelná a vyjádřená za použití jednoduchých jazykových prostředků. Souhlas se zpracováním musí zahrnovat i konkrétní účel, pro který je dáván. Účel musí být dostatečně specifikován, aby z něj subjekt údajů získal představu o tom, jak bude s jeho osobními údaji nakládáno. V případě, že by byl účel vymezen příliš obecně či vágně, je pravděpodobné, že souhlas nebude dostatečně konkrétní.

Aby byl souhlas se zpracováním svobodný, nesmí být jeho udělení podmínkou např. pro uzavření smlouvy, poskytnutí služby apod., pokud není takové zpracování pro plnění ze smlouvy či poskytnutí služby zcela nezbytné. Jeho neudělení nesmí mít pro subjekt údajů žádné negativní následky. Např. pokud chce internetový obchodník zasílat zákazníkům nabídky zboží, reklamu apod., nesmí podmiňovat dodávky objednaného zboží udělením takového souhlasu ke zpracování údajů pro účely zasílání nabídek, reklam apod. Samotnou dodávku zboží dle smlouvy lze totiž realizovat i bez zasílání nabídek zboží, k plnění ze smlouvy není zasílání nabídek nezbytné. Zákazník musí mít skutečnou a reálnou možnost souhlas s užitím údajů pro účely nabídek a reklam neudělit a přitom si zachovat možnost dále zboží nakupovat.

S tím souvisí i zásadní novinka, a to požadavek **na odlišitelnost souhlasu** od jiných skutečností, k nimž se subjekt údajů rovněž vyjadřuje. **Souhlas musí být oddělený od smlouvy, obchodních podmínek; není možné, aby byl jejich součástí.** Pokud by totiž byl jejich součástí (jak to dosud bylo v praxi běžné), pak vlastně subjekt nemá možnost volby souhlas (se zasíláním nabídek) neudělit, ale zároveň akceptovat obchodní podmínky pro nákup zboží. Takový souhlas je neplatný a je třeba ho získat znovu za podmínek dle GDPR. Dalším příkladem, kdy je předpoklad svobodně uděleného souhlasu slabší, je udělení souhlasu subjektem ve slabším postavení (např. zaměstnanec ve vztahu k zaměstnavateli, občan ve vztahu k orgánu veřejné moci).

Informovaný je souhlas tehdy, pokud subjekt údajů obdržel před jeho udělením veškeré informace podle článku 13 GDPR (např. totožnost a kontaktní údaje správce, účely zpracování a právní základ zpracování, doba, po kterou budou údaje uloženy, existence práva požadovat přístup k údajům, opravu, výmaz apod.). Tyto údaje musí být navíc sděleny transparentně, srozumitelně a za použití jasných a jednoduchých jazykových prostředků.

Souhlas musí být udělen zjevným potvrzením. To však neznamená, že by musel být výslovný**.** Postačí, pokud subjekt údajů učiní nějakou akci, ze které je zjevné, že má v úmyslu souhlas udělit. Může se jednat o zaškrtnutí políčka (které by však nemělo být zaškrtnuto předem) či podpis, ale např. také o vyplnění e-mailové adresy do pole, u kterého je uvedeno, že si subjekt údajů přeje zasílat reklamní sdělení. Uvedené však neplatí pro citlivé osobní údaje, kde v souladu se stávající právní úpravou zůstal zachován požadavek výslovnosti.

Souhlas musí být kdykoli odvolatelný, o tom musí být subjekt údajů informován. Odvolání souhlasu musí být stejně snadné jako jeho poskytnutí.

Odvolání souhlasu nemusí pro správce znamenat nutně povinnost údaje zlikvidovat, jelikož odvolání souhlasu se děje k určitému účelu, pro který jsou osobní údaje zpracovávány, přičemž správce může osobní údaje zpracovávat pro jiné účely, pro které využije jiný právní důvod zpracování než je souhlas subjektu údajů. Pokud však takový jiný důvod nenajde, je povinen údaj zlikvidovat.

Souhlasy musí být v souladu s nařízením GDPR. Stávající souhlasy budou platné a použitelné jen za předpokladu, že odpovídají právní úpravě v nařízení GDPR. Jde-li ve Vašem případě o zpracování osobních údajů, ke kterému je třeba souhlas, doporučujeme dosavadní způsob udílení souhlasů přezkoumat a případně si vyžádat od subjektů souhlasy nové.

GDPR a marketing

GDPR v bodu 47 svého odůvodnění stanoví, že *„zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu“*. Do určité (avšak patrně velmi malé) míry je možné osobní údaje pro účely přímého marketingu zpracovávat i bez souhlasu subjektů údajů. Tato výjimka však bude podle převažujících názorů naopak vykládána spíše restriktivně. Oprávněný zájem správce je tedy třeba v každém případě samostatně posoudit a bude dán zejména tam, kde existuje relevantní a odpovídající vztah mezi subjektem údajů a správcem, např. pokud je subjekt údajů dlouholetým zákazníkem správce. Klíčové pro posouzení oprávněného zájmu je zejména to, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít.

Správce a zpracovatel, smlouva o zpracování osobních údajů

Pokud osobní údaje, např. svých zákazníků nebo zaměstnanců správce předá někomu jinému (zpracovateli), aby s těmito údaji pracoval, je nutné mít písemně upravena práva a povinnosti správce při takovém zpracování - uzavřít písemnou smlouvu o zpracování osobních údajů, která musí mít náležitosti dle článku 28 GDPR, popř. tyto náležitosti zahrnout do smlouvy o hlavní činnosti prováděné zpracovatelem pro správce (např. o poskytování služeb). Jinak by správce pro předání údajů jiným osobám mimo firmu musel získat souhlas subjektů údajů (pokud nejde o požadavek policie nebo jiného státního orgánu, který má právo si údaje potřebné pro svoji činnost vyžádat a je povinnost mu je poskytnout). Typickým příkladem, kdy dochází ke zpracování osobních údajů zpracovatelem pro správce a je třeba mít písemně upravena pravidla zpracovávání dle článku 28 GDPR, je situace, kdy zaměstnavateli (správci) zpracovává mzdovou agendu zaměstnanců popř. účetnictví externí firma (zpracovatel). V rámci plnění (hlavní) smlouvy o vedení mzdové agendy či účetnictví nakládá účetní firma s osobními údaji zaměstnanců správce (správce jí je předává a určuje účel zpracovávání). Vedle pravidel pro zpracovávání účetnictví je tedy třeba smluvně písemně upravit pravidla pro zpracovávání osobních údajů mezi správcem (zaměstnavatelem) a zpracovatelem (účetní firmou). Lze uzavřít samostatnou smlouvu o zpracování osobních údajů nebo pravidla zahrnout do hlavní smlouvy, vždy však musí být obsaženy náležitosti dle článku 28 GDPR.

Pravidla, zásady, povinnosti

1. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být vždy **přiměřené účelu** zpracování.

2. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno **férově, korektně a transparentně.** Informace o zpracování poskytované subjektu údajů musí být zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci.

3. Zpracování nesmí nadměrně **zasahovat do soukromí**. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.

4. Po naplnění účelu zpracování je dána povinnost osobní údaje **zlikvidovat**. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).

5. Rozsah zpracovávaných údajů by měl být **jen minimální** (nezbytný) pro dosažení daného účelu. Správce musí dbát, aby získávané údaje byly přesné a jejich přesnost ověřovat.

6. Údaje by měly být uchovávány jen po **nezbytně dlouhou dobu**. Ta doba se může v různých případech hodně odlišovat. Ne vždy končí doba nutná k uchovávání všech údajů ukončením nějaké činnosti, např. ukončením pracovního poměru nebo naplněním smluvního ujednání. V úvahu je třeba brát jak lhůty stanovené zákonem pro uchovávání některých dokumentů, tak případné promlčecí lhůty pro možnost podání soudní žaloby a v případě listinných dokumentů i lhůty skartační.

7. Subjekty údajů mají svá práva, která musí správce respektovat. Mezi ně patří právo na poskytnutí **informací** o svých údajích. Již při získávání údajů je třeba dotyčnému subjektu údajů poskytnout informace dle článku 13 GDPR, nejlépe v písemné podobě, ať již v místě, kde k získání údajů dochází nebo i prostřednictvím webových stránek. Subjekt má právo i na poskytnutí kopie svých údajů. K dalším právům patří právo na **opravu** nepřesných údajů, právo **vznést námitku**, např. proti dalšímu zasílání marketingových nabídek, a také právo na **výmaz** údajů, ale pouze pokud není jiný důvod pro jejich další uchovávání.

8. Osobní údaje je nutné **zabezpečit.** Listinné dokumenty musí správce uchovávat např. v uzamčené zásuvce stolu nebo v uzamčené skříni a neponechat je v neuzamčené místnosti, pokud z ní odchází ten, kdo s nimi má pracovat. K údajům uloženým v počítači nebo jiném elektronickém zařízení může mít na základě správně zvoleného hesla přístup vždy jen ten, kdo je pověřen, aby s určitými údaji pracoval. U větších a složitějších systémů je také třeba pořizovat elektronické záznamy, které umožňují určit a ověřit, kdy, kdo a z jakého důvodu údaje používá, tzv. logy.

Pravidla bezpečnosti je třeba zachovávat i u elektronických prostředků používaných při různých cestách, např. je neponechávat bez dozoru v automobilu. Osobní údaje musejí být odpovídajícím způsobem zabezpečeny i při jejich přenosu elektronickými prostředky. Běžná e-mailová komunikace není považována za příliš bezpečnou. V některých případech je tak vhodné zvolit bezpečnější formu přenosu informací obsahujících osobní údaje. Vždy je nutné zvážit vhodnost zasílání nikterak nezabezpečených dokumentů obsahujících větší penzům osobních údajů (či citlivých) prostřednictvím freemailových služeb. Neznamená to však, že by nebylo možné nikdy použít freemailovou službu, např. pokud jde jenom o jednoduchou domluvu se zákazníkem či zaslání nikterak rizikových informací.

9. Správce má však i další povinnosti. Obecně mají všichni správci povinnost **vést záznamy o činnostech**, které se s osobními údaji provádějí. Lze doporučit připravit si na to formulář s kolonkami a do nich zapsat informace požadované v článku 30 GDPR (záznam o evidenci smluv, o evidenci zaměstnanců, případně o slevovém programu pro zákazníky aj.).

Další obecně platnou povinností všech správců je povinnost **ohlašování případů porušení zabezpečení osobních údajů** Úřadu pro ochranu osobních údajů podle článku 33 GDPR (do 72 hodin od zjištění takového incidentu). Hlásit je třeba závažné incidenty s předpokládanými závažnými důsledky.

Naopak povinnost jmenovat **pověřence** pro ochranu osobních údajů dopadá jen na některé správce či zpracovatele, a to na tyto případy:

a) zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů jednajících v rámci svých soudních pravomocí);
b) hlavní činnosti správce nebo zpracovatele spočívají ve zpracování údajů, které vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů;
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a údajů týkajících se rozsudků v trestních věcech a trestných činů;

Patrně sem budou patřit tedy i školy, nemocnice, zdravotnická zařízení.

Stejně jako jmenování pověřence není ani **posouzení vlivu na ochranu osobních údajů a předchozí konzultace s Úřadem pro ochranu osobních údajů** povinností obecně platnou, týká se těch, kdo hodlají provádět s osobními údaji rozsáhlé rizikové operace, spočívající například v rozsáhlém profilování lidí prostřednictvím internetu, při kterém jsou pro marketingové účely získávány podrobné informace o jejich soukromém životě, nebo rizikovost spočívá ve využití nových technologií používaných, např. na velké množství údajů o zdravotním stavu pacientů. Seznam těchto operací bude Úřadem pro ochranu osobních údajů zveřejněn.

Sankce

Flagrantního porušení obecným nařízením stanovených povinností při takových rizikových operacích prováděných ve velkém objemu dat, zpravidla velkými nadnárodními společnosti, se mohou týkat maximální, obecným nařízením stanovené sankce, dosahující značných částek. Případné sankce za porušení povinností obecného nařízení budou dle vyjádření Úřadu pro ochranu osobních údajů jako dosud přiměřené a v žádném případě nemohou být likvidační.

V případě, že byste měli k dané problematice dílčí dotazy, neváhejte se na nás obrátit. Pokud byste si přáli komplexní služby auditu a navazující implementace pravidel ochrany údajů dle GDPR u Vás ve firmě, jsme připraveni Vám doporučit na tuto problematiku specializované odborníky a poskytnout k tomu potřebnou právní podporu.

S pozdravy a úctou

Mgr. Dana Cirkovská
advokát

JUDr. Filip Hruška
advokát