GDPR aneb ochrana osobních údajů v praxi

Úvod, který je nutné přečíst! Bezpodmínečně.

GDPR je zkratka, která se běžně používá ve veřejném prostoru, vycházející z anglického „General Data Protection Regulation“. V podstatě nejde o nic jiného než o ochranu osobních údajů, což v rámci ČR bylo řešeno zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. V současnosti (od 25.5.2018) se ochrana osobních údajů řeší podle obecného nařízení Evropského parlamentu a Rady Evropské unie 2016/679 /dále jen GDPR nebo nařízení/ (1) a v souladu s ním zpracovaným našim zákonem o zpracování osobních údajů č. _____/20___ Sb. (pozn. k 30.4.2018 Zákon dosud nebyl přijat, později proto doplnit ručním vepsáním.)

GDPR lze nalézt zde :

https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=CS

Jakékoli zákony, nařízení vlády, vyhlášky …, lze nalézt např. zde www.zakonyprolidi.cz , když si ovšem uvědomíme, že jakékoli závazné znění je obsaženo jen a jen ve Sbírce zákonů.

GDPR pak dopadne i osoby samostatně výdělečně činné (OSVČ), či osoby právnické (a.s., s.r.o., k.s., družstva), ale i jiné, dále i souhrnně označovaní jako „tito“/„tyto“. I tyto zpracovávají osobní údaje a z hlediska GDPR to jsou správci osobních údajů (čl. 4/7 nařízení). Lidé, jejichž osobní údaje tito zpracovávají, jsou subjekty osobních údajů (čl. 4/1 nařízení). Více k pojmosloví v rámci GDPR čl. 4 nařízení. Za tím účelem tedy musejí tito zpracovánu příslušnou dokumentaci. GDPR se naopak netýká činnosti fyzické osoby, viz čl. 2, odst. 2, písm. c) nařízení, při kterých jsou zpracovávány osobní údaje výlučně pro osobní či domácí činnost.

Problematika osobních údajů je čím dál komplikovanější a čím dál více sledovaná. Pokuta za porušení ochrany osobních údajů může být relativně „likvidační“. Naštěstí podle judikatury ve skutečnosti pokuty likvidační být nesmějí. Ovšemže je tedy v bytostném zájmu odpovědných osob, mít vše kolem, a nejen kolem, GDPR v bytostném pořádku.

Pro práci s jakýmkoli textem týkajícím se GDPR je dobré, spíš nutné, mít u ruky nařízení a příslušné zákony.

Radostné sdělení! Méně byrokracie.

Na začátek by bylo dobré si říct něco ohledně dokumentace, kterou tito díky GDPR musí disponovat. Tak předně tito nemají, ani nebudou mít, oznamovací povinnost vůči Úřadu na ochranu osobních údajů o tom, že zpracovávají anebo budou zpracovávat osobní údaje (viz. §18/1c) zákona č. 101/2000 Sb., který ovšem účinností GDPR, a nebude-li nahrazen jiným, ztratí na významu). Ono totiž nařízení oznamovací povinnost zrušilo (tím, že ji nezavedlo), i když ji z části nahradilo povinností vést záznamy o činnostech zpracování. Záznamy o činnostech zpracování by se však těchto týkat nemusely, pokud nemají 250 zaměstnanců či více anebo např. nezpracovávají určité údaje, kvůli kterým by je vést musel /rasa, náboženství atd./, čl. 30 nařízení. Oznamovací povinnost nařízení z další části nahradilo konzultacemi s Úřadem na ochranu osobních údajů v případě vysokého rizika pro osobní údaje, čl. 36 nařízení, což se vzhledem k následujícímu odstavci nejspíše většiny těchto, netýká, většina zaměstnavatelů zaměstnává, alespoň se domnívám do 250 osob. Každopádně tento text je určen těm, kteří toto kriterium splňují a zaměstnávají do 250 osob. Viz. k tomu i bod 88 v úvodu nařízení, ještě před čl. 1 (tedy bod č. 88 v recitálu). Pokud, nedej Bože, by někdo nějak dovodil, že záznamy o činnostech zpracování se týkají i těchto, pak pro tento případ, lze za tyto záznamy považovat i text „Prohlášení o ochraně osobních údajů“ nebo i jednotlivé „Informační listy“, které požadované obsahují bez ohledu na to, jak se jmenují.

Na začátek by bylo dobré si též říct, že nařízení stanoví ve svém čl. 35 povinnost, v některých případech, provést tzv. „Posouzení vlivu na ochranu osobních údajů“, což není nic jiného, než jakási analýza rizik při zpracování osobních údajů, samozřejmě byrokraticky náročná. Tak tedy dobrá zpráva je, tito, míněno nyní malé podnikatele a firmy, toto provádět nemusejí. Zcela jistě se totiž naštěstí nevejdou do uvedených parametrů. To proto, že na otázku, která zní : „Je pravděpodobný následek vysokého rizika pro osobní údaje ve smyslu čl. 35/1, 2, 3) nařízení?“, lze v případě řady subjektů, které nezpracovávají osobní údaje např. automatizovaně nebo přímo ve www

rozhraní, odpovědět jednoznačně : „Ne!“. Z této odpovědi tedy vyplyne, že posouzení vlivu na ochranu osobních údajů není potřebné.

Proč ne? Protože někteří, snad většina, neprovádí „systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad; ani rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 (údaje o rasovém, etnickém původu atd.) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; a ani rozsáhlé systematické monitorování veřejně přístupných prostorů“; a jak k nyní uvedené citaci z čl. 35 nařízení dodávám já, neprovádí ani jakékoli zpracovávání osobních údajů, způsobem, který by tyto mohl ohrozit. Zpravidla je uchovávají doma v PC a v účetnictví. K jejich zabezpečení pak více jinde.

Takže Posouzení vlivu na ochranu osobních údajů zpracovat nemusí a fakt zpracovávání osobních údajů také hlásit na nějaký úřad nemusí!

<u>Co tedy udělat nejdřív? Více byrokracie.</u>

Jde především o to, že tito, jako správci osobních údajů, si v prvé řadě musí opatřit nařízení a eventuálně náš zákon k němu, bude-li, a několik dalších zákonů či vyhlášek! A dále :

1. Učinit si přehled o tom jaké osobní údaje tito zpracovávají (to může být např. jméno nebo příjmení, adresa pobytu, rodné číslo, datum narození, e-mailová adresa, telefonní číslo, RZ automobilu, fotografie, atd., atd., v podstatě cokoli podle čeho se dá, ať již přímo či nepřímo, identifikovat konkrétní osoba. Definice je v čl. 4/1 nařízení.
2. Určit proč osobní údaje zpracovává (evidence zákazníků, evidence účetních dokladů atd., atd., atd.), a je-li zpracovávání z těchto důvodů nezbytné.
3. Je nutné si k údajům přiřadit právní titul, na základě kterého jsou zpracovávány. Tímto právním titulem je vše, co je vyjmenované v čl. 6 nařízení a jde o 6 základních důvodů. Pro tyto půjde především o plnění právní povinnosti, plnění smlouvy nebo na základě souhlasu subjektu údajů. I když souhlas subjektu by měl být až tím posledním, čím zpracování odůvodnit, protože souhlas lze kdykoli odejmout (více k souhlasu i čl. 7 nařízení). Dále to mohou být i situace ochrany životně důležitých zájmů subjektu údajů nebo jiné osoby, nebo i splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci. Formulace jsou to sice vágní a jejich vysvětlení, pokud vůbec existuje, v textu nařízení je doprovázeno slovy zejména, přiměřeně apod., takže rozšiřující výklad těchto pojmů by byl možný. Zde, v tomto kroku, tedy doložíme sami sobě, potažmo kontrole, zda osobní údaje zpracováváme z důvodů, které jsou v souladu s legislativou, tedy pouze v souladu s účelem, který plyne z nařízení, z čl. 6.
4. Dále je potřeba stanovit lhůtu, po jakou tyto údaje zpracovávat chce/musí. To plyne z jiných právních předpisů (např. zákon o účetnictví - § 31 a 32, z trestního zákoníku – 40/2009 Sb. /promlčecí doba různých TČ např. krácení daně atd., je různá, zpravidla 5 nebo 10 let/ anebo plyne prostě pouze z účelu, který si tito stanovili, a pro který je údaj zpracováván a zde bude nutný souhlas subjektu údajů.
5. Musí též dle předchozího připravit poučení, přesněji splnit svoji informační povinnost (čl. 13 nařízení), ve vztahu k subjektu údajů, jehož údaje chce/musí zpracovávat a toto „šité na míru“ zjištěním z kroků 1 až 4. Takový dokument musí obsahovat povinné náležitosti (čl. 12, 13 a 14 nařízení a dále i čl. 15, 16, 17, 18, 20). A to transparentně, srozumitelně, dostupně, stručně, pokud lze o stručnosti, či srozumitelnosti, díky požadavkům GDPR, vůbec hovořit.

Musíme si uvědomit, že „Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů tyto informace“ … (čl. 13 nařízení). Tedy musíme si uvědomit, že jakmile osobní údaje dostáváme, tak musíme splnit tam uvedené povinnosti. Podle mne nejlépe tím, že subjektu údajů předáme dokument, který ve svém obsahu toto zajistí, a takové převzetí si necháme stvrdit podpisem, z důvodu naší právní jistoty, neboť v dnešní době jedině co je psáno, to je dáno ... Ovšem postačí např. zaslání e-mailem, ale zde bych doporučoval odeslaný e-mail vytisknout a uschovat po dobu, po jakou budou osobní údaje

dotčené osoby zpracovávány, a nebo kupř. na dodejku poštou s tím, že bych vytisknul poučení a dodejku k němu přilepil a obé uschovával po dobu, po jakou budou osobní údaje dotčené osoby zpracovávány. Dodejka má podobu korespondenčního lístku.

6. Pokud jde o osobní údaje zpracovávané i elektronicky, pak musí být zajištěna např. i záložní elektronická kopie (čl. 32/1c nařízení). Případně tyto údaje i šifrovat (recitál č. 83 nařízení). Např. pomocí volby hesla ve Word, Excel, a nebo části či celého HDD v PC např. pomocí programu TrueCrypt atd.

7. V případě, že tito chtějí údaje zpracovávat pouze na základě souhlasu subjektu údajů, musí též připravit souhlas subjektu údajů, podle požadavků čl. 4/11 a 7 nařízení.

Zcela namístě by pak bylo opatřit si i např. www stránky s odkazem na problematiku osobních údajů a zde vyřešit způsob nakládání s osobními údaji, informovanost, poučení atd. komplexně. Stejně tak to může být učiněno vyvěšením např. na nástěnce v sídle, v krajním případě eventuálně umožněním nahlédnout do dokumentace v kanceláři v sídle po domluvě, ale zde bych měl trochu pochybnost, zda tímto je plně splněn požadavek na dostupnost. A i na toto umístění odkazovat v dokumentech, které se předají osobě, která osobní údaje poskytla. Toto komplexní zpracování nazvat např. „Prohlášení o ochraně osobních údajů“ obdobně, jako to dělávají velké firmy a jako to udělám i já.

Zřízení www stránek nemusí být až takový problém. Cena je různá a jde o cca 1.500,- Kč ročně za pronájem www.

Ještě návrat k „Záznamům o činnostech zpracování“ (čl. 30/1 a 2) nařízení). Záznamy o činnostech zpracování, zpravidla, tito, podle mne, nepovedou, nemají zpravidla 250 zaměstnanců či více anebo např. nezpracovávají určité údaje, kvůli kterým by je vést museli /rasa, náboženství atd./, čl. 30 nařízení, obdobně konzultace. Zde lze znovu uvést, že např. OSVČ nebude nucen provádět posouzení vlivu na ochranu osobních údajů (čl. 35 nařízení), tudíž nebude ani muset na základě jeho výsledku vést s úřadem konzultace. Vždyť čl. 30 odst. 5) nařízení zní doslova „Povinnosti uvedené v odstavcích 1 a 2 se nepoužijí pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.“ I s přihlédnutím k textu, který je uveden v recitálu č. 76 a 83 nařízení, se lze dotázat - „Proč by např. OSVČ museli vést záznamy o činnostech zpracování?“ Vždyť např. OSVČ naprosto jasně, zpravidla, není podnik a ani organizace, která by zaměstnávala 250 či více osob, tedy naopak např. OSVČ je, zpravidla, zcela jasně organizace, která zaměstnává méně než 250 osob. Zpravidla např. OSVČ zaměstnává přesně nula osob. Např. OSVČ tedy, zpravidla, nezaměstnává 250 či více zaměstnanců. To za prvé. Za další, jaké riziko pro práva a svobody představuje zpracovávání údajů např. OSVČ pro subjekt údajů, to i v kontextu který je uveden v recitálu č. 76 a 83 nařízení? Zcela zanedbatelné, když srovnáme s internetovým obchodem nebo bankou. Na čí servery hackeři útočí, které seznamy, záznamy, informace chtějí, truhlářské, vinařské? To asi ne. Tak tedy musí se vést záznamy, protože zpracování osobních údajů není příležitostné? Např. OSVČ, malé firmy, kupříkladu truhláři nebo vinaři, přece neshromažďují údaje plánovitě, ale právě příležitostně. Při získání zákazníka, či jeho platbách, tedy jen při vybraných příležitostech a nikoli systematicky, plánovitě, např. jen pro samé získávání osobních údajů pro marketingové účely. A již vůbec se zpracování údajů ze strany např. OSVČ, zpravidla, netýká zvláštních kategorií údajů čl. 9/1 nařízení /rasa, náboženství atd./, a samozřejmě spolek nepracuje v rámci rozsudků v trestních věcech … Takže proč vést záznamy o činnostech zpracování? Ten důvod zatím nevidím. Je to náš národní sport být „papežštější než papež“, ale není to nutné!

Ještě k pojmu organizace. Tento pojem není v nařízení definován, na rozdíl od mezinárodní organizace (čl. 4/26). Lze tedy vyjít z obecného vnímání tohoto slova a to je takové, že organizace je slovo, pod nímž rozumíme jednak organizovanou a formální skupinu lidí, kteří mají společné cíle a jsou vymezeni vůči okolnímu prostředí a jednak činnost – organizování. My toto slovo v kontextu

shora uvedeného chápeme jako skupinu osob se společným cílem. Organizací pak může být např. nějaká vládní organizace, mezinárodní organizace, nezisková organizace, politická strana, profesní komora anebo spolek, atd. S pojmem organizace, mezinárodní organizace nebo sdružení nařízení pracuje vedle sebe. Prostě kompatibilita našich předpisů a evropských není pojmově 100%, ale co nám brání v tom, vykládat je v náš prospěch? Nic. Zvláště tehdy nic, když nařízení ve svém čl. 4/18 nařízení deklaruje, že se rozumí „podnikem jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost;“. Co z toho plyne? Že např. OSVČ, s.r.o., je, zpravidla, podnikem, který nezaměstnává 250 a více osob atd. atd. tak, jak jsem již napsal shora a tudíž nemusí vést záznamy o činnostech zpracování tak, jak jsem již také shora napsal.

A na věci nic nemění ani to, že nařízení pracuje s pojmy podnik (tento pojem definuje), organizace (tento pojem nedefinuje) i sdružení (tento pojem přímo nedefinuje) a jakoby tedy činilo rozdíl mezi organizací, podnikem a sdružením. Jenže to je problém těch co nařízení sestavovali a nikoli náš, že nemají jasno v tom, jak lze vykládat různé pojmy. Čeština je prostě bohatý jazyk, v Bruselu zcela jistě málo užívaný …

Prohlášeni o ochraně osobních údajů

Na základě nařízení a přehledu, který jsme si učinili v rámci osobních údajů, které jako tito zpracováváme, můžeme nyní přistoupit k vytvoření dokumentu, který můžeme nazvat např. „Prohlášení o ochraně osobních údajů“, tak, jak to i nyní řeší různé firmy, a jak to provedu já. A dále i k vytvoření dokumentu, nazývám jej „Informační list“, který předáme subjektu údajů v okamžiku, kdy jeho osobní údaje získáváme.

V textu „Prohlášení o ochraně osobních údajů“ budu propojovat články z nařízení, vyvedené modrým písmem s vlastním textem v černé barvě a tam, kde bude prostor pro doplnění jiných údajů, budu vkládat text červený. Červený text lze vymazat anebo nahradit textem jiným. Černý či modrý text zůstává. Nařízení je nutné mít při ruce; to eventuálně i další předpisy. Vše v tom prohlášení uvedené je samozřejmě jen možností, jak si věci uspořádat a navíc, jak s oblibou vždy zdůrazňuji ... „Jde o můj právní názor. Rozhodující slovo v případě jakéhokoli sporu je věcí soudní soustavy ČR.“

Zmíněné „Prohlášení o ochraně osobních údajů“ či „Informační list“ lze tedy přizpůsobit. To je prozatím vše.

S pozdravem

Mgr. Milan FENDRICH
administrativní pracovník
fi. Voneš-stavby s.r.o.