Aktuální informace o GDPR pro neziskové organizace a malé firmy

Běžné nestátní neziskové organizaci nebo živnostníkovi nepřináší Nařízení Evropského Parlamentu a Rady 2016/679 (GDPR) příliš komplikací. Drtivá většina NNO a malých firem nemusí mít speciální software pro zabezpečení zpracování osobních údajů, nemusí jmenovat pověřence pro ochranu osobních údajů a pokud nemá více než 250 zaměstnanců, nemá ani povinnost vést záznamy o činnostech zpracování osobní údajů.

Výklady tohoto nařízení jsou ale i necelé tři měsíce před jeho účinností velmi odlišné. Je to dáno jeho obecností, mnohdy nepochopením základních pojmů, ale zejména komerčními zájmy některých poradenských firem, které v aplikaci GDPR vidí nový zdroj svých příjmů.

V České republice toto nařízení z velké části odpovídá právní úpravě podle stávajícího **zákona č. 101/2000 Sb., o ochraně osobních údajů. A kdo se tímto zákonem řídí již dnes, nemusí tedy mít z GDPR obavy.**

Audit zpracování osobních údajů si zvládne malá organizace udělat sama. V něm jde o to si ujasnit, jaké kategorie osobních údajů organizace zpracovává a k jakému účelu, kdo s nimi pracuje, kde jsou uloženy a jak jsou chráněny. Výstupem pak budou vnitřní směrnice o zpracování osobních údajů, které budou popisovat základní povinnosti organizace - "správce". Mnohé povinnosti jsou stejné nebo velmi podobné těm, které už musíme plnit podle zákona č. 101/2000 Sb., o ochraně osobních údajů.

A které povinnosti to například jsou?

Ujasnit si z jakých zákonných důvodů osobní údaje zpracováváte. Souhlas "subjektu osobních údajů", tedy člověka, kterého se týkají, je jen jedním, nejméně preferovaným z důvodů, jež ke zpracovávání opravňují – nejčastěji totiž půjde o zpracování na základě zákona, zpracování nutné ke splnění smluvních povinností nebo pro účely oprávněných zájmů příslušného správce.

Text tohoto souhlasu je třeba aktualizovat, protože GDPR stanovuje mírně odlišně od současné úpravy podmínky toho, kdy je souhlas musí být jednoznačný, srozumitelný, svobodný, konkrétní a informovaný. Tento doplněný souhlas budou podepisovat až noví klienti, zaměstnanci, dobrovolníci, **stávající souhlasy zůstávají platné, pokud jsou svým obsahem a formou v souladu s požadavky GDPR.** Mimochodem, víte, že souhlas s pořizováním a zveřejňováním fotografií a videozáznamů už je popsán v občanském zákoníku? Není to tedy také žádná nová povinnost.

Organizace či firma si musí si také uvědomit, jakou kategorii údajů zpracovává. **Citlivé údaje, nově zvláštní kategorie údajů,** se stejně jako dříve obecně zpracovávat nesmí, vyjma několika účelů v GDPR přímo uvedených. Patří mezi ně mimo jiné i zdravotní a sociální péče. **Osobní údaje dětí** se smí zpracovávat jen se souhlasem zákonného zástupce. Tady je nutné vyčkat schválení zákona o zpracování osobních údajů, který přesně určí věkovou hranici pro tento souhlas. V návrhu je prozatím stanovena na 13 let, starší děti by tedy mohly souhlas již udělovat samy.

Práva subjektů jsou již také velmi podobně popsána ve stávajícím zákoně č.101/2000 Sb., známe **právo na přístup k údajům, na opravu údajů i na výmaz, tedy na**

"zapomenutí". Nově přibude **právo na omezení zpracování a na přenositelnost údajů** - zde zdůrazňuji, pokud je to technicky proveditelné.

Pokud pro "správce" osobní údaje někdo zpracovává, je třeba se **dohodnout na aktualizaci smlouvy se zpracovatelem,** aby její znění odpovídalo nařízením GDPR. Zvláště, pokud jde o přeshraniční zpracovávání. Což mimochodem může být i v případě, že máte údaje uložené na cloudu.

Výstupem z auditu pak bude vnitřní směrnice, popisující všechny procesy zpracování osobních údajů, nezbytnou dobu pro jejich uchování, odpovědné osoby a program jejich proškolování, technologie zpracování, zabezpečení a prevenci rizik, postupy při informování subjektů, a také případně dozorového orgánu, pokud dojde porušení zabezpečení údajů.

Tento text není přesný "návod k použití" ani neměnný výčet povinností. Každá organizace, firma či podnikatel jsou jiní, a to velikostí, činností, počtem zaměstnanců, klientelou a technickým vybavením. Každý se tedy musí novému nařízení přizpůsobit trochu jinak.

Některé změny může ještě přinést nový zákon o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb. a bude "prováděcím zákonem" GDPR. Nicméně GDPR bude platit, i když tento zákon nebude včas schválen.

Nechejte si poradit, ale nenechte se vystrašit. Informace získávejte od více zdrojů a porovnávejte. Doporučuji je ale získávat od firem a poradců, kteří vám v souvislosti s poskytnutými radami nebudou nabízet nějakou další navazující komerční službu.

Bc. Milada Šnajdrová
tel. 776 13 33 72, mail@miladasnajdrova.cz
www.miladasnajdrova.cz

V Olomouci dne 13. března 2018