Povinnosti NNO vyplývající z *"Nařízení Evropského Parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES"* (GDPR)

Nařízení Evropského Parlamentu a Rady 2016/679, GDPR (dále Obecné nařízení) je nový zákon na ochranu osobních údajů, účinný ve všech zemích EU od 25. května 2018. V České republice tak toto Obecné nařízení nahradí stávající zákon č. 101/2000 Sb., o ochraně osobních údajů, a v konkrétních detailech ho doplní ho nový připravovaný zákon o zpracování osobních údajů.

Výklady Obecného nařízení se prozatím různí. Je to dáno jeho obecností a možností konkretizace v některých detailech metodikou každé země, mnohdy nepochopením základních pojmů a bohužel i komerčními zájmy některých IT a poradenských firem, které v aplikaci GDPR vidí nový zdroj svých příjmů.

V České republice má vzniknout **dozorový úřad,** který bude mít v gesci regulaci GDPR, metodickou podporu a kontrolu dodržování pravidel. V tuto chvíli je neformálním poradním místem Úřad na ochranu osobních údajů (ÚOOÚ), který se také s největší pravděpodobností stane tímto dozorovým úřadem.

V tomto textu chci uvést na pravou míru některé články na internetu, nabídky komerčních společností a až katastrofické informace, šířící se neziskovým sektorem. Vycházím z informací ÚOOÚ a konzultací se špičkovými právníky a IT odborníky.

I sám ÚOOÚ je při posuzování dopadu ve srovnání se současnou úpravou spíše zdrženlivý:
"Je nutné zdůraznit, že základní zásady, principy a klíčové instrumenty zůstávají de facto neměnné. ... *Obecné nařízení na těchto základech přináší nástavbu spočívající v dodatečných nových povinnostech, které pro české správce budou nové.*
Jde zejména o tyto nové povinnosti:

1. *povinnost vést záznamy o činnostech zpracování*
2. *posouzení vlivu na ochranu osobních údajů*
3. *předchozí konzultace*
4. *ohlašování případu porušení zabezpečení osobních údajů dozorovému úřadu*
5. *oznamování případu porušení zabezpečení osobních údajů subjektu údajů*
6. *ustavení pověřence pro ochranu osobních údajů"*[1]

Většiny NNO se v praxi týkají pouze tři body, tedy body **4. a 5., a k bodu 1.** uvádím, že povinnost vést záznamy se podle Obecného nařízení týká organizací zaměstnávajících **více než 250 zaměstnanců.**

Pro upřesnění uvádím i **popis některých základních pojmů Obecného nařízení:**

[1] Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích, Úřad na ochranu osobních údajů, dostupné na: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=23790

Zpracováním osobních údajů ve smyslu Obecného nařízení je míněna rozsáhlá činnost, kterou správce s osobními údaji provádí za určitým účelem a systematicky.

Subjekt, který tímto způsobem zpracovává osobní údaje, se nazývá **správce. Zpracovatelem** je subjekt, který dle pokynů správce osobní údaje technicky zpracovává.

Existují **právní důvody** zpracování osobních údajů, přičemž nejdůležitějším a v praxi nejpoužívanějším je a zůstává zpracování na základě zákonného oprávnění (např. pro účely ochrany práv, plnění zákonných povinností nebo plnění smlouvy s fyzickými osobami). U dětí do 13 let (jak uvádí návrh nového zákona) je třeba souhlasu rodičů.

Obecné nařízení vymezuje podmínky, za kterých tyto údaje smí být zpracovány **zvláštní kategorie osobních údajů** (v zákoně 101/2000 Sb., o ochraně osobních údajů, označené jako "citlivé"), nestanovuje však žádná další opatření při nakládání s těmito údaji. Doporučuje se pouze zvýšená ochrana těchto údajů.

Interní audit není komplikovaný proces, na který je nutné povolat (a platit) auditorskou firmu. Jde jen o to si ujasnit, a nejlépe ve vnitřním předpisu popsat, jaký druh osobních údajů se zpracovává, kdo s nimi pracuje, kde jsou uloženy, zda má organizace prokazatelný souhlas subjektu údajů, k jakému účelu jsou data zpracovávána, po jakou dobu, kde a jak se osobní údaje archivují atd. Tento přehled si zvládne každá NNO udělat sama.

Obecné nařízení ustanovuje **Pověřence pro ochranu osobních údajů.** Pověřence musí jmenovat správce a zpracovatel pokud:

- zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí,
- hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
- hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech.

Veřejný subjekt není naším zákonem prozatím přesně popsán, ale jeho vymezení se nesmí odchýlit od vymezení EU, kde se jedná např. o armádu, policii, soudy a další instituce, přes které uplatňuje stát svou moc, případně zařízení s rozsáhlým zpracováním citlivých údajů.

Nestátní neziskové organizace tak pověřence mít skutečně nemusí, ač vám to možná budou tvrdit některé komerční subjekty, které nabízí pověřence jako externí službu.

K další údajné povinnosti všech organizací **pořídit si specializovaný software,** uvádí ÚOOÚ[2], že:

"Obecné nařízení neukládá povinnost použít pro zabezpečení zpracování některé specifické opatření."

[2] [2] Desatero omylů o obecném nařízení (GDPR), Úřad na ochranu osobních údajů, dostupné na: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=23799

V praxi tak platí, že **v naprosté většině případů týkajících se NNO pro naplnění povinností vyplývajících z Obecného nařízení zcela postačí stručná směrnice o zpracování osobních údajů, dobře vedený archiv a běžné zabezpečení sítě,** což jsou věci, kterými by NNO měly disponovat již dnes.

A nyní mi dovolte několik praktických rad:

- přesto, že je už nyní velký mediální a zejména komerční tlak na zavádění opatření ke GDPR, **neuspěchejte přípravu**. Zjišťujte si informace od více zdrojů a zejména od zdrojů, které vám na základě podaných informací nebudou nabízet komerční službu.
- přijměte změnu zákona jako podnět ke zmapování způsobů nakládání s osobními údaji. **Udělejte si vlastní interní audit** zpracovávání osobních údajů, který bude probíhat podle vašich konkrétních potřeb a jasných, nejlépe předem sepsaných pravidel. Nastavte si případně nové, bezpečnější způsoby nakládání s údaji, zejména s citlivými údaji.
- na základě auditu si pročistěte databáze údajů, zbavte se bezpečným způsobem těch, které už nepotřebujete. Získejte souhlasy těch, kteří vám je dosud neposkytli, pokud je potřebujete (získejte právní důvod nakládání s údaji).
- **popište si případná rizika** při ochraně osobních údajů a najděte způsoby, jak je eliminovat.
- připravte se i na právo člověka "být zapomenut" a nastavte si mechanizmy bezpečného vymazání dat na případné vyžádání subjektu údajů.
- pokud nezpracováváte velké množství osobních údajů nebo dokonce citlivých údajů, **nepotřebujete žádný nový drahý software** nebo specializované konzultační služby.
- **NNO nemají povinnost mít pověřence pro ochranu osobních údajů.**
- vyčkejte s definitivními rozhodnutími na **schválení českého zákona o zpracování osobních údajů a vydání závazných metodických pokynů** novým Dozorovým úřadem.

Bc. Milada Šnajdrová
poradce pro NNO a expert na neziskový sektor ČR
tel. 776 13 33 72, mail@miladasnajdrova.cz
www.miladasnajdrova.cz

V Olomouci dne 2. září 2017