Obecné nařízení o ochraně osobních údajů

Naše znalosti pro Váš úspěch

ÚOOÚ,
kontroly, sankce ve vztahu ke GDPR

JUDr. Jiří Žůrek

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Obecné nařízení (GDPR) ve zkratce

- Účelem je sjednotit evropský rámec ochrany osobních údajů při jejich zpracování
  - Postaveno na stejných základních kamenech jako směrnice 95/46/ES, avšak doplněno o princip odpovědnosti správce a přístup založený na riziku a s ním spojené nové povinnosti
  - Zvýšená ochrana subjektu údajů
  - Více sjednocený evropský dozor, nové role dozorových úřadů

Obecné nařízení (GDPR) ve zkratce

- Jednotný evropský právní rámec = jednotný právní výklad napříč Evropou
  - Významná role pracovní skupiny WP29, resp. Sboru
  - Možnost vydávat metodické výklady k některým institutům v Obecném nařízení, již nyní existují 4 vodítka a vodítko k ohlašování případu porušení zabezpečení by mělo být dostupné v říjnu

Dozorový úřad –
Úřad pro ochranu osobních údajů

- Každý členský stát má za povinnost ustanovit nezávislý **dozorový úřad**
  - Splněno bude v adaptačním zákoně, který je nyní v přípravě
    - Pracovně nazýván zákon o zpracování osobních údajů

- V České republice je a bude dozorový úřad –
  Úřad pro ochranu osobních údajů

Dozorový úřad –
Úřad pro ochranu osobních údajů

- V GDPR stanoveny tyto úkoly (čl. 57)
  - **Monitoruje a vymáhá uplatňování nařízení**
  - Poskytuje informace subjektům údajů ohledně výkonu jejich práv
  - **Zabývá se stížnostmi, které podá subjekt údajů nebo organizace, která jej zastupuje**
  - Spolupracuje s ostatními dozorovými úřadu
  - Podporuje vydávání kodexů, schvaluje kodexy

(pozn.: jde o výňatek, nikoli o kompletní výčet)

Čl. 31 GDPR – Správce a zpracovatel spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů

Dozorový úřad –
Úřad pro ochranu osobních údajů

- Za účelem plnění úkolů, může využít pravomoci (čl. 58):
  - **Vyšetřovací**
    - Zejména možnost provést kontrolu
  - Nápravné
    - Např. udělit napomenutí
  - Povolovací a poradní
    - Např. schvalovat kodexy chování

Dozorový úřad –
Úřad pro ochranu osobních údajů

- Vyšetřovací pravomoci dle GDPR
  - **Nařídit správci a zpracovateli, aby poskytli veškeré informace nutné ke splnění úkolů**
  - **Provádět vyšetřování formou auditu (tj. kontrolu)**
  - Provádět přezkum osvědčení k akreditaci
  - Ohlásit správci nebo zpracovateli údajné porušení GDPR

Dozorový úřad –
Úřad pro ochranu osobních údajů

- Samotný výkon kontroly se řídí zákonem **č. 255/2012 Sb., o kontrole (kontrolní řád)**
  - Upravuje především procesní hledisko prováděné kontroly
  - Práva/povinnosti kontrolujícího
  - Práva/povinnosti kontrolovaného

Dozorový úřad –
Úřad pro ochranu osobních údajů

- Účel kontroly
  - Kontrolní orgán při kontrole zjišťuje, jak kontrolovaná osoba plní povinnosti, které jí vyplývají z jiných právních předpisů nebo které jí byly uloženy na základě těchto předpisů.
  - Ideálně, pokud kontrolou neshledáno žádné porušení.

Co když je shledáno porušení?

- Pokud shledáno porušení, je možné dle GDPR uplatnit některou z **nápravných pravomocí** a to např.:
  - Udělit správci napomenutí
  - Nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv
  - Nařídit správci nebo zpracovateli uvést zpracování do souladu s Obecným nařízením
  - Nařídit správci, aby subjektu údajů oznámil případ porušení zabezpečení osobních údajů
  - Uložit pokutu dle článku 83 vedle či **namísto** jiných nápravných opatření

(pozn.: jde o výňatek, nikoli o kompletní výčet)

Podmínky pro ukládání pokut dle GDPR

- Správní pokuty se ukládají podle okolností každého případu
  - Rozhodně není účelem stanovení vysokých sankcí likvidace organizací
- Sankce mají především preventivní, odstrašující a donucující účinek

Podmínky pro ukládání pokut

- Při rozhodování o tom zda uložit správní pokutu, a případně jakou výši, se zohledňují např. tyto okolnosti:
  - Povaha, závažnost, délka trvání porušení s přihlédnutím k povaze, rozsahu a účelu zpracování, jakož i k počtu dotčených subjektů údajů
  - Kategorie dotčených osobních údajů
  - Úmysl či nedbalost
  - Kroky podniknuté správcem ke zmírnění škod
  - Předchozí porušení správce
  - Míra spolupráce s dozorovým úřadem
  - Dodržování kodexu, osvědčení
  - Okolnosti, jak se Úřad dozvěděl o porušení, zda mu jej správce oznámil

Podmínky pro ukládání pokut

- Za „méně závažná“ porušení lze uložit správní pokutu až do výše 10 000 000 EUR, nebo jedná-li se o podnik až do výše 2% celkového ročního obratu

- Za závažnější porušení lze uložit správní pokutu do výše 20 000 000 EUR nebo do 4% celosvětového ročního obratu

Podmínky pro ukládání pokut

- Byť výše pokut vypadá hrozivě, je důležité zmínit, že pokud správce bude přistupovat ke zpracování osobních údajů **svědomitě**, takto vysoké sankce mu s největší pravděpodobností nehrozí

- Dobrá zpráva pro správce: Nikoli za každé porušení musí být udělena pokuta
  - V úvahu přichází i upozornění či napomenutí nebo jiné nápravné opatření

Obecné nařízení

- Není to strašák, ale příležitost uvést zpracování do souladu, věnovat se mu
- Střízlivě posoudit prováděné zpracování s povinnostmi dle Obecného nařízení
- Brát řádné zpracování jako konkurenční výhodu
  - Možno podpůrně i kodexy a osvědčení
- Nezapomenou na zaměstnance
- Střízlivě posuzovat nabídky zázračných softwarů GDPR ready

Kam míří Vaše pozornost,
tam směřuje Vaše energie,
a tam se objeví i výsledky

=

GDPR

Děkuji za pozornost!

JUDr. Jiří Žůrek

Tuto konferenci pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz