Úřad pro ochranu osobních údajů
v době účinnosti GDPR

Seminář „Ochrana osobních údajů ve firmách v době účinnosti GDPR“

30. 10. 2018
Ostrava

JUDr. Jiří Žůrek
ředitel odboru konzultačních agend

GDPR ve zkratce I.

- GDPR je **přímo účinné** pro jeho adresáty ve všech členských státech
  - Hlavními adresáty jsou **správci**, zpracovatelé, subjekty údajů a dozorové úřady
- Sjednocení evropského rámce ochrany osobních údajů při jejich zpracování k zamezení nedůvodného tříštění stanovených pravidel vnitrostátním zákonodárstvím
- **Stejné základy** jako měla směrnice 95/46/ES (resp. zákon č. 101/2000 Sb.), avšak doplněno o **princip odpovědnosti správce** a **přístup založený na riziku** a s ním spojené některé nové povinnosti
  - Některé nové povinnosti zakládají i nové činnosti ÚOOÚ
- Zvýšená ochrana subjektu údajů
- Více sjednocený evropský dozor, nové role dozorových úřadů

GDPR ve zkratce II.

- GDPR je tzv. performance based regulation
  - Nestanovuje všechny povinnosti plošně na všechny správce či zpracovatele, ale v závislosti na činnostech zpracování se na některé správce vztahují dodatečné povinnosti (např. mít jmenovaného pověřence, provést posouzení vlivu na ochranu osobních údajů)
  - Každý správce či zpracovatel si tak musí stanovit, jak se jej GDPR dotkne
  - Běžného živnostníka či výrobní společnosti se GDPR vesměs dotkne ve stejném rozsahu jako zákon č. 101/2000 Sb.

  - **Základy** – zejména zásady zpracování, zabezpečení osobních údajů – musí plnit každý

  - **Vše se odvíjí od účelu zpracování**

GDPR ve zkratce III.

- Možnost v některých ustanovení se odchýlit vnitrostátním zákonodárstvím
- Současně je nutno připravit právní řád české republiky na dopad GDPR, které nebylo přijímáno českým zákonodárcem a tudíž je nutné pro něj připravit „půdu“ v ČR
- Též je nutné na zákonné bázi ustanovit dozorový úřad, jeho organizaci s ohledem na GDPR atd.

  - Shora uvedené má být obsahem tzv. adaptačního zákona, který doposud nebyl přijat (sněmovní tisk č. 138)

- Absence adaptačního zákona se může dotýkat některých správců (spíše z řad veřejné správy) a výrazněji dozorového úřadu, tj. ÚOOÚ
- Nelze akceptovat obecné výmluvy, není adaptační zákon, nebudu se řídit GDPR

Úřad pro ochranu osobních údajů (ÚOOÚ)

- Každý členský stát má podle GDPR za povinnost ustanovit nezávislý **dozorový úřad**
- V České republice **je** a **bude** dozorový úřad **ÚOOÚ**
- Do přijetí adaptačního zákona je jeho ustavení a organizace upravena stále, v tomto rozsahu, platným a účinným zákonem č. 101/2000 Sb., o ochraně osobních údajů
- Od účinnosti adaptačního zákona bude ustavení a organizace ÚOOÚ upravena adaptačním zákonem

ÚOOÚ v době účinnosti GDPR

- GDPR ovlivnilo nejen správce a zpracovatele, ale i ÚOOÚ

- Co zůstalo stejné?
  - „Klasická“ role dozorového úřadu (**stížnostní, kontrolní agenda**) = monitorování a vymáhání uplatňování GDPR

- Co je pro ÚOOÚ nové?
  - **Data breaches** (oznámení porušení zabezpečení oú)
  - **Předchozí konzultace**
  - **„Evidence“ oznámení o kontaktních údajích na pověřence**
  - **Činnosti při přijímání kodexů chování**
  - **Zrušení oznamovací povinnosti** – registr oznámení „zanikl“

Stížnostní agenda ÚOOÚ

- Co se děje s podnětem a jak na Vás může přijít **kontrola**?:

  - **Podněty/stížnosti** – ÚOOÚ se zabývá především stížnostmi subjektů údajů
    - Pokud je podnět/stížnost vyhodnocen jako relevantní pro kontrolu (tj. jde o závažnou věc, nutnou ověřit i kontrolně) **=** kontrola
    - V případě, že je (závažnější) porušení doloženo = zpravidla správní řízení
    - **V méně závažných případech porušení je přistoupeno k zaslání informace správci a očekává se, že správce drobné porušení sám napraví – stovky takových upozornění ročně**
    - Pokud podnět/stížnost nejsou vyhodnoceny jako důvodné = sdělení stěžovateli s důvody odložení, včetně doporučeného postupu

  - **Kontrolní plán** – každoročně se vypracovává s vymezením oblasti či druhu správců či zpracovatelů, kteří se zkontrolují

  - **Medializovaný „průšvih“** – pokud se ÚOOÚ něco dozví např. z médií, není vyloučen pokyn předsedkyně k zahájení kontroly

Stížnostní agenda ÚOOÚ

- **Jak na sebe neupozornit?**
  - ➢ Dodržovat GDPR ☺
    - Plnit práva subjektu údajů – velmi často se stává, že správce nevyhoví či vůbec neodpoví subjektu údajů = zaslaná stížnost na ÚOOÚ

- **Nejčastější předmět stížností:**

  - ➢ Kamerové systémy – např. instalace bez vědomí zaměstnanců

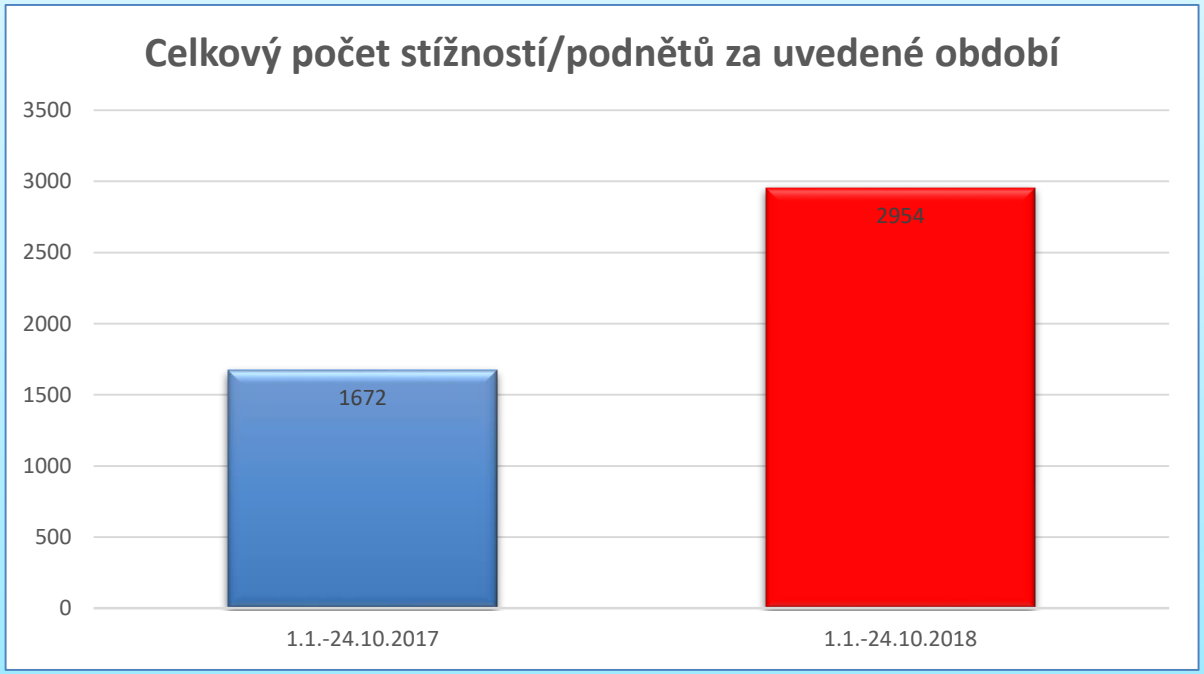
  - ➢ Výkon práv subjektu údajů - např. neuspokojení subjektu údajů v rámci přístupu k osobním údajům

  - ➢ Telemarketing – např. obtěžování s telemarketingovými hovory

  - ➢ Zejména u některých velkých správců způsob získávání souhlasu – např. agresivní formou

Porovnání doby před a po účinnosti GDPR

- Medializace tématu GDPR a ochrany osobních údajů vyústila ve zvýšený počet stížností



Kontrolní činnost

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

- **Účelem kontroly** je zjistit faktický stav, zahájení kontroly ≠ automaticky zjištění porušení či udělení pokuty

- Kontrolu lze vést v některých případech i korespondenčně
- Ideálně, pokud není shledáno žádné porušení

Kontrolní činnost

- Pokud shledáno porušení, je možné dle GDPR uplatnit některou (a to i více z nich) 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

Podmínky pro ukládání pokut podle GDPR

- Sankce mají především **preventivní**, **odstrašující** a **donucující** účinek
  - Snahy některých zákonodárců zmírnit či úplně vyloučit pokuty pro veřejnou správu v adaptačním zákoně.
    - Byl by takový krok správný?
- Správní pokuty se ukládají podle okolností každého případu
  - Rozhodně není účelem stanovení vysokých sankcí likvidace organizací

Podmínky pro ukládání pokut podle GDPR

- 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 podle GDPR

- 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 podle GDPR

- 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

- Nikoli za každé porušení musí být udělena pokuta
  - V úvahu přichází i upozornění či napomenutí nebo jiné **nápravné opatření**

Absence adaptačního zákona a kontrolní/sankční činnost

- Důsledky jsou jak organizační, tak i funkční, do určité míry i ovlivňující „represivní“ část činnosti ÚOOÚ
- **Kontroluje** se dodržování povinností jak dle GDPR, tak i jednání před účinnosti GDPR podle zákona č. 101/2000 Sb.
- Udělování pokut „není na pořadu dne“ (není však vyloučeno), pokutují se především porušení, která se stala ještě za plné účinnosti zákona č. 101/2000 Sb. (tedy za porušení do 24. 5. 2018 včetně).
- Do určité míry lze tento stav „právního vakua“ využít jako druhou šanci uvést zpracování do souladu

Nové agendy ÚOOÚ v souvislosti s GDPR

Ohlašování porušení zabezpečení osobních údajů

- **Nová** povinnost pro správce (viz článek 31 GDPR)
  - Jde o povinnost vztahující se eventuálně na všechny správce
  - Předmětem povinnosti je ohlásit dozorovému úřadu **rizikový** případ porušení zabezpečení osobních údajů pro práva a svobody fyzických osob

- **Informace k této povinnosti viz www.uoou.cz + pokyny Sboru**

- Z oznámení musí vyplývat určité skutečnosti, které GDPR stanovuje
- **Důležité body** – popis opatření, které správce přijal nebo navrhl s cílem vyřešit dané porušení zabezpečení osobních údajů + pravděpodobné důsledky pro subjekty údajů

- **Role ÚOOÚ** = vyhodnocení přijatých ohlášení
  - Není účelem každé přijaté ohlášení podrobovat kontrole či sankci
  - Evropská spolupráce u přeshraničních porušení zabezpečení

Statistika „data breaches“

- Velká část se týká „hackerských“ útoků, typu ransomware či zapomenutých zařízení
  - Zálohování, šifrování často zmírní možná rizika = tj. není mnohdy ani nutné oznamovat

- Od počátku této povinnosti obdrženo **170 ohlášení**, z toho jich 15 bylo dále řešeno (včetně spolupráce s ostatními dozorovými úřady)
  - Porušení zabezpečení se děje jak v soukromí tak i veřejné sféře
  - Mnohdy oznamovány i banality či strohé oznámení, bez všech povinných náležitostí (zejména chybí popis opatření či pravděpodobné důsledky)

Předchozí konzultace

- „Institucionalizovaná“ konzultace
  - Pouze v případech, kdy z posouzení vlivu, které správce provedl, přetrvává i přes přijetí opatření ke zmírnění rizika, vysoké riziko pro práva a svobody subjektu údajů
  - Nelze zaměňovat s konzultační či osvětovou agendou ÚOOÚ
- K dnešnímu dni ještě předchozí konzultace ve smyslu čl. 36 GDPR **nevedena**

„Evidence“ kontaktních údajů na pověřence

- **Pouze** evidenční charakter, **nikoli** registrační
  - Spíše než o evidenci, jde o příjem ohlášení ze strany správců a zpracovatelů
  - Nejde o evidenci pověřenců jako takových
  - Nezveřejňuje se
- Účelem je usnadnit kontakt dozorového úřadu se správcem či zpracovatelem
- Cca 16 800 správců a zpracovatelů sdělilo kontaktní údaje na pověřence
- Jsou zastoupeni jak interní, vlastní pověřenci, tak i externí
- **Pozor** zejména u advokátů či jiných osob na možný střet zájmů

Činnost u kodexů chování

- Kodexy chování jsou institut výrazně spojený s principem odpovědnosti správce
  - Jejich vznik je předpokládán na sektorové úrovni
- Přihlášením ke kodexu správce a priori deklaruje soulad zpracování
  - **Není povinností se hlásit ke kodexu, ani jej vypracovat**
- Aby měl kodex váhu, musí jej schválit autorita = dozorový úřad
  - S ÚOOÚ lze úvahy o kodexu konzultovat, včetně již probíhajících prací
- Monitorování souladu zpracování s kodexem
  - ÚOOÚ v rámci svých úkolů a pravomocí
  - ÚOOÚ akreditovaný subjekt k monitorování kodexu chování

Zrušená oznamovací povinnost

- V současném světě neefektivní povinnost, pozbyla účelu
- Správci **již neoznamují** zpracování dozorovému úřadu
- Již není aktivní registrační formulář
- Zaregistrovaná oznámení nadále dostupná, nicméně vypovídající hodnota s časem klesá
- Úvahy, že po přijetí adaptačního zákona bude registr dostupný cca rok a půl
- Náhrada: záznamy o činnostech zpracování, posouzení vlivu na ochranu osobních údajů

Pár slov ke konzultační činnosti

Konzultační činnost

- Medializace tématu GDPR a ochrany osobních údajů vyústila ve zvýšený počet dotazů

Konzultační činnost

- Přímá konzultační činnost na běžné dotazy je v GDPR upozaděna (ve srovnání se zákonem č. 101/2000 Sb.) – „náhrada“ byla poskytnuta ve formě velkého množství informací zveřejněných na www.uoou.cz.
  - Mimo jiné i podstatně přebudována **rubrika často kladených otázek**
  - Zřízena **telefonní informační** linka pro správce
  - **Účas**t zástupců i na seminářích v regionech

- Prvotní roli pro konzultace správce či zpracovatele přejímá pověřenec (tam kde byl jmenován)

- Nelze opominout ani roli gesčních ministerstev při tvorbě metodik či různých profesních sdružení, komor atd.

- Konzultační role ÚOOÚ tak spočívá zejména u předchozích konzultací nebo u jiných složitějších záležitostí

- GDPR (obecné nařízení)
- Poradna
- Povinně zveřejňované informace
- Právní předpisy
- Judikatura
- Dozorová činnost
- Nevyžádaná obchodní sdělení
- Veřejný registr zpracování osobních údajů
- Předávání osobních údajů do třetích zemí
- Zahraničí
- Informační systémy EU (Schengen)
- Informační systém ORG
- Publikace
- Pro mládež

Novinky

K povinnosti jmenovat pověřence vybranými městskými a krajskými organizacemi

19. 10. 2018 – Úřad pro ochranu osobních údajů zveřejňuje podrobnější informace týkající se rozsahu povinnosti jmenovat pověřence některými městskými či krajskými organizacemi.

Často kladené otázky k předávání osobních údajů do třetích zemí

10. 10. 2018 - Úřad pro ochranu osobních údajů uveřejnil na svých webových stránkách časté otázky z oblasti předávání osobních údajů do třetích zemí.

Aktualizace informací v případu portálu ZnamyLekar.cz

4. 10. 2018 - Úřad pro ochranu osobních údajů zveřejňuje aktualizované informace ke zpracování osobních údajů portálem www.znamylekar.cz.

Úřad udělil společnosti Internet Mall, a.s. pokutu 1,5 milionu korun

3. 10. 2018 - Úřad pro ochranu osobních údajů uložil na základě závěrů kontroly pokutu ve výši 1,5 milionu korun společnosti Internet Mall, a.s. Důvodem bylo, že firma nezabezpečila osobní údaje nejméně 735 tisíc zákazníků.

Zpracování politických názorů voličů pro kampaň je možné jen s jejich souhlasem

2. 10. 2018 – Úřad pro ochranu osobních údajů v souvislosti s nadcházejícími říjnovými volbami do Senátu a obecních zastupitelstev připomíná, že údaje vypovídající o politických názorech občanů patří do zvláštní kategorie osobních údajů, pro které GDPR (článek 9) stanovuje zákaz jejich zpracování s přísně stanovenými výjimkami.

GDPR (obecné nařízení)

- GDPR stručně
- Základní příručka k GDPR
- Kodexy chování
- Desatero zpracování pro správce
- Záznamy o činnostech zpracování
- Porušení zabezpečení
- Pověřenci
- Desatero omylů
- Dokumenty k GDPR
- Otázky a odpovědi
- Pokyny Sboru
- GDPR nově
- Role ÚOOÚ
- Důležité odkazy
- MIKROWEB K GDPR

Poradna

- Často kladené otázky podle oblastí
- Chci podat stížnost na správce nebo zpracovatele (formulář PDF)
- Kamerové systémy, kamera souseda
- Mám dotaz. Jak postupovat?
- Slovníček nejdůležitějších pojmů
- Základní informace pro e-shopy

Jak konzultovat?

- Pokud nenaleznete odpověď na stránkách ÚOOÚ či případně na stránkách gesčního ministerstva/sdružení/asociace tak zaslaný dotaz by měl splňovat určitá kritéria
  - Měl by obsahovat popis dotazu/věci
  - Vaší analýzu problému, jak byste jej řešili, jak jej vidíte
  - Návrh řešení

- Shora uvedené výrazně zvýší šance, že bude dotaz odpovězen v přiměřené době mezi záplavou dalších dotazů (malá připomínka: kapacity jsou primárně určeny na stížnosti jelikož ÚOOÚ = **dozorový** úřad).

Děkuji Vám za pozornost