HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

www.komora.cz

Nová pravidla ochrany osobních údajů

JUDr. Markéta Schormová
Úřad Hospodářské komory České republiky

25.5.2017

PROČ NOVÁ EU LEGISLATIVA?

- Směrnice z roku 1995 neodpovídá technologickému pokroku v oblasti ICT - sociální sítě, internetové nabídky a služby, online obchody = rozsáhlý sběr a zpracování OÚ, monitorování a profilování FO
- Nová evropská právní úprava: forma nařízení = přímo aplikovatelná pravidla
- Cílem zajistit jednotný režim ochrany v celé EU
- Příprava nových pravidel: 4 roky a přesto již zastarávají – např. internet věcí – zavádění chytrých zařízení denní potřeby zasahuje do osobních údajů

GDPR – General Data Protection Regulation

- Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (**obecné nařízení o ochraně osobních údajů**), kterým se zrušuje směrnice 95/46/ES.
- Účinnost od 25. 5. 2018
- Nejkomplexnější soubor pravidel na ochranu dat
- Novela zákona č. 101/2000 Sb., o ochraně osobních údajů - procesní norma, novelizace – léto 2017?

GDPR

- Základní principy právní úpravy beze změn
- Podrobnější a přísnější pravidla správcům a zpracovatelům
- Přesnější úprava fyzických osob
- Dozor – Úřad na ochranu osobních údajů

NA KOHO SE PRAVIDLA GDPR VZTAHUJÍ? SANKCE?

- všechny firmy v EU, které nabízí zboží a služby rezidentům EU a při své činnosti zpracovávají osobní údaje

- zpracování osobních údajů – jakákoli operace (i automatizovaná) spočívající ve shromažďování, ukládání, strukturování, vyhledávání či výmazu

- sankce: dnes 10 mil. Kč x nově až 10/20 mil. eur, resp. 2/4% z celosvětového obratu

KRITÉRIA PRO UKLÁDÁNÍ SANKCÍ

- Úmysl x nedbalost
- Závažnost a délka porušení s přihlédnutím k povaze, rozsahu, účelu zpracování
- Počet poškozených FO
- Vzniklá škoda
- První nebo opakované porušení
- Součinnost s dozorovým orgánem
- Opatření k nápravě – technická, personální

Nová definice osobních údajů?

- **Osobními údaji se dle GDPR rozumí:**

„veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.

Nová definice osobních údajů?

- Zůstává zachována kategorie citlivých osobních údajů: př. rasový původ, náboženské vyznání, zdravotní stav
- Jsou součástí definice – biometrické údaje (např. scan sítnice, otisk prstu), genetické údaje (např. DNA)
- Nejsou součástí definice – údaje zesnulých osob a anonymizované údaje
- Nově též ochrana osobních údajů dětí (13/16/18 let)
- Vždy je třeba osobní údaje zpracovávat v souladu s účelem zpracování!
- Nepotřebné údaje smazat!

OSOBNÍ ÚDAJE – ZÁSADY ZPRACOVÁNÍ

- zákonnost, korektnost, transparentnost
- pouze pro daný účel
- právní tituly k nakládání s OÚ:
  - souhlas: vědomý, svobodný, konkrétní
    NE předvyplněná políčka
  - plnění smlouvy
    NE souhlas vložit do smlouvy
  - právní povinnost (např. zaměstnavatel)
  - veřejný zájem (např. policie)

Správce x zpracovatel

- **správce** = ten (FO/PO), kdo určuje účel a způsob zpracování
- **zpracovatel** = FO/PO, která zpracovává osobní údaje jménem správce – typicky poskytovatel služeb: mzdová agenda, IT a cloudové služby
- stávající pravidla – nejsou povinnosti pro zpracovatele, plná odpovědnost správce
- nová pravidla – správce i zpracovatel přímá odpovědnost za řádné zpracování osobních údajů

Nové povinnosti správců I.

- zabezpečení osobních údajů - porušení ochrany dat musí být oznámeno do 72 hodin – ÚOOÚ + FO (např. hackerský útok na zabezpečení bankovních hesel)
- vnitřní předpisy – kodexy chování, záznamy o činnostech, pověřenec, školení zaměstnanců, kontrola
- nastavení technických opatření – např. šifrování dat, pseudonymizace (nahrazení jména číslem)
- oznámení není nutné, pokud by porušení zabezpečení OÚ pravděpodobně nemělo za následek riziko pro práva a svobody FO

Nové povinnosti správců II.

- vést záznamy o činnostech zpracování – povinnost pouze pro firmy zaměstnávající nad 250 osob, pokud jejich hlavní činnosti není zpracovávání OÚ

- posouzení vlivu na ochranu OÚ – **před** zahájením zpracování + pravděpodobnost vysokého rizika pro práva a svobody FO (možnost konzultace s ÚOOÚ)
  - systematické a rozsáhlé vyhodnocování osobních aspektů FO založené na automatizovaném zpracování
  - rozsáhlé systematické monitorování
  - typicky telekomunikační společnosti, dodávky energií

Nové povinnosti správců III.

- pověřenec pro ochranu OÚ - výklad. stanovisko ÚOOÚ
  - Povinnost jmenovat pouze pro orgány veřejné moci – metodika Ministerstva vnitra
  - Hlavní činnosti správce spočívají v operacích zpracování, které kvůli povaze, rozsahu nebo účelům vyžadují rozsáhlé pravidelné a systematické monitorování FO
- úkoly pověřence: poskytování informací a poradenství, monitorování souladu s GDPR, odborná příprava pracovníků, spolupráce s ÚOOÚ

Nejen nová práva fyzických osob

- právo na přístup k OÚ + na informace od správce
- právo na opravu + právo vznést námitku
- právo na výmaz – vždy, když pomine účel zpracování, při odvolání souhlasu, při protiprávním zpracování
- právo na přenositelnost OÚ k jinému správci – ve strukturovaném, běžně používaném a strojově čitelném formátu (včetně metadat) – výkladové stanovisko ÚOOÚ
- **POZOR!** Porušení práv FO ze strany správců = porušení, za která jsou nejvyšší sankce.

e-privacy I.

- Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života o ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 200/58/ES (**nařízení o soukromí a elektronických komunikacích**)

- předložen EK 10.1.2017, přidělen výborům v EP
- účinnost květen 2018?
- nahradí stávající směrnici o soukromí a elektronických komunikacích, která se vztahuje na tradiční telekomunikační operátory

e-privacy II.

- předsednictví Estonska v Radě 2. pol. 2017 – zřejmě politický tlak na rychlé projednání
- novela zákona č. 480/2004 Sb., o některých službách informační společnosti
- novela zákona č. 127/2005 Sb., o elektronických komunikacích

e-privacy III.

- Nová pravidla pro poskytovatele služeb elektronických komunikací – např. Facebook, Skype, Viber, WhatsApp
- Ochrana dat nejen u obsahu, ale též u metadat odvozených od elektronické komunikace (např. čas a místo hovoru)
- Jednodušší pravidla týkající se cookies – nebude vyžadován souhlas, neboť cookies nezasahují do soukromí a zlepšují služby internetu
- Výraznější ochrana proti spamu

VÍCE INFORMACÍ NA WEBU HK ČR:

http://www.komora.cz/pro-podnikani/legislativa-a-normy/aktuality-z-legislativy/obecne-narizeni-na-ochranu-osobnich-udaju.aspx

Děkuji za pozornost.

Hospodářská komora České republiky, Florentinum (recepce A), Na Florenci 2116/15, 110 00 Praha 1
T: 266 721 300, F: 266 721 690, E: office@komora.cz