STRUČNÁ INFORMACE OHLEDNĚ NOVÉ EVROPSKÉ PRÁVNÍ ÚPRAVY OCHRANY OSOBNÍCH ÚDAJŮ

V návaznosti na přípravu na nabytí účinnosti nového Obecného nařízení o ochraně osobních údajů č. 2016/679/EU (General Data Protection Regulation - „**GDPR**“) si tímto dovolujeme poskytnout stručnou informaci ohledně možných změn a případných požadavků souvisejících se zajištěním souladu s GDPR, jak následuje. S ohledem na skutečnost, že bližší informace budou průběžně zveřejňovány ze strany Úřadu pro ochranu osobních údajů a dalších subjektů, lze následně přikročit k poskytnutí detailnějšího vhledu do předmětné problematiky.

I.
Úvodní informace

- GDPR nabude účinnosti dne **25. května 2018;**
- Týká se subjektů, které zpracovávají data třetích osob, a to ve vztahu k dokumentům v elektronické i papírové podobě (aktuální zejména ve vztahu k internetovým obchodům nebo spotřebitelským soutěžím);
- Má přispět k zajištění stejné úrovně a vymahatelnosti ochrany osobních údajů ve všech členských státech Evropské Unie;
- V některých ohledech přináší povinnosti nad rámec stávající právní úpravy, resp. nové přístupy k ochraně osobních údajů, nicméně vychází ze shodných základů a jeho prostřednictvím dochází ke zpřesnění úpravy příslušných práv a povinností;
- **Správcem osobních údajů** je podle GDPR každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí za jím stanoveným účelem jejich shromažďování, zpracování a uchování;
- **Zpracovatelem osobních údajů** je subjekt, který jménem správce zpracovává osobní údaje (na základě smlouvy uzavřené se správcem);
- S účinností GDPR odpadne povinnost registrace správce/zpracovatele osobních údajů u Úřadu pro ochranu osobních údajů; nově ale vznikne oznamovací povinnost vůči ÚOOÚ při narušení bezpečnosti údajů (např. hackerský útok) do 72 hodin od okamžiku, kdy se správce o narušení dozví.

II.
Výběr z právní úpravy zakotvené GDPR

- Bude možné získat osvědčení o souladu zpracování osobních údajů s povinnostmi zakotvenými GDPR ze strany akreditovaného subjektu - v současné době probíhají práce na stanovení formy a postupů pro akreditaci;

- **Zpřesnění definice osobních údajů**
  - Za stanovených podmínek je osobním údajem i e-mailová adresa, telefonní číslo, IP adresa, tzv. cookies v zařízení uživatele;

- Přísnější režim stanoven pro citlivé údaje (rasový/etnický původ, politické názory, náboženské vyznání, členství v odborech zdravotní stav, sexuální orientace, delikty) a biometrické údaje (osobní údaje technického charakteru, sem spadá i snímek obličeje či podpis osoby);
- Údaje, které **nepožívají ochrany** při zpracování:
  - údaje právnických osob,
  - anonymizované údaje,
  - osobní údaje zemřelých osob,
  - údaje získané v rámci činnosti čistě osobní povahy.

- Základem pro oprávněné zpracování osobních údajů je prokazatelný a informovaný **souhlas subjektu se zpracováním osobních údajů**; existuje však samozřejmě řada případů, u nichž není souhlasu se zpracováním osobních údajů třeba - např. plnění právních povinností ve vztahu k subjektu údajů, plnění povinností vyplývajících ze smlouvy (předání doručovacích údajů dopravci) apod.
- Žádost o vyjádření souhlasu se zpracováním osobních údajů musí být samostatná - odlišitelná od obchodních podmínek, resp. souhlasu subjektu s obchodními podmínkami (např. v rámci objednávky v e-shopu je třeba označit samostatné políčko ohledně souhlasu se zpracováním osobních údajů ve stanoveném rozsahu a vytvořit informaci o zpracování a ochraně osobních údajů oddělenou od textu obchodních podmínek, v níž bude mj. sděleno, komu budou získaná data případně poskytována, za jakým účelem a na jak dlouho).
- Souhlas se zpracováním osobních údajů získaný v rozporu se shora uvedenými informacemi (např. pouze v rámci souhlasu s obchodními podmínkami) by pro další zpracovávání předmětných osobních údajů mělo být třeba získat od subjektu osobních údajů znovu.

- **Povinnosti správců/zpracovatelů osobních údajů**
  - **Tzv. princip odpovědnosti** – povinnost zavést příslušná technická, organizační a procesní opatření za účelem zajištění souladu s principy GDPR a zároveň povinnost zajištění souladu v případě kontroly doložit (jak je zajištěna bezpečnost osobních údajů, jaké osoby k nim mají přístup, zda např. existuje vnitřní směrnice o nakládání s osobními údaji);
  - Rozsah zavedených opatření závisí na množství a účelu zpracování osobních údajů a riziku, které příslušné zpracování osobních údajů nebo porušení zabezpečení představuje;
  - Zavedení opatření, která dodržují zásady záměrné a standardní ochrany osobních údajů – zpracovávání pouze nezbytně nutného množství osobních údajů po nutnou dobu, transparentnost s ohledem na účely a způsob zpracování osobních údajů;
  - Důkladné informování subjektů osobních údajů o způsobu zpracovávání osobních údajů a souvisejících právech (blíže specifikováno v odstavci ohledně práv subjektu údajů);
  - **Vedení záznamů o činnostech zpracování** – ty musí obsahovat:
    - jméno a kontaktní údaje správce/zpracovatele;
    - účely zpracování (např. zasílání obchodních sdělení);
    - popis kategorií subjektů údajů a kategorií osobních údajů;
    - kategorie příjemců, kterým byly nebo budou údaje zpřístupněny;
    - informace o mezinárodním předávání osobních údajů;

- lhůty pro výmaz jednotlivých kategorií údajů;
- popis technických a organizačních opatření k zabezpečení osobních údajů (heslo, omezení přístupu k ukládaným osobním údajům apod.)

(Záznamy není třeba vést v případě subjektu s méně než 250 zaměstnanci, ledaže zpracování osobních údajů ze strany uvedeného subjektu představuje riziko pro práva a svobody osob, není příležitostné, nebo se týká citlivých údajů.)

- V některých případech je třeba jmenovat pověřence pro ochranu osobních údajů (týká se orgánů veřejné moci, subjektů, jejichž hlavní činnosti vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů - např. poskytovatelé telekomunikačních služeb - nebo jejichž hlavní činnosti spočívají v rozsáhlém zpracování specifikovaných citlivých údajů).

- **Práva subjektů údajů (osob, kterým údaje patří):**
  - Musí být o svých právech důkladně informováni (před udělením souhlasu se zpracováním osobních údajů)
    - Právo vznést námitku proti zpracování údajů, pokud správce nemá prokazatelné důvody pro jejich další zpracování;
    - Právo na přenositelnost osobních údajů od jednoho správce k druhému, pokud jsou údaje zpracovávány automatizovaně a zpracování je založeno na souhlasu nebo na smlouvě;
    - Právo na přístup k údajům, které jsou o subjektu shromažďovány – informace, zda jsou osobní údaje subjektu zpracovávány, a pokud ano, pak pro jaké účely apod.;
    - Právo na opravu údajů, na omezení zpracování (v určitých vymezených případech);
    - Právo na výmaz („právo být zapomenut“) – není-li zpracování údajů již potřebné pro původní účel, odvolá-li subjekt souhlas, vznese-li subjekt námitku proti zpracování z oprávněných zájmů, při protiprávním zpracování osobních údajů, pokud chybí rodičovský souhlas se zpracováním osobních údajů dětí, právní povinnost stanovená státem nebo EU (většina případů je stanovena i stávající právní úpravou). Odvolat souhlas se zpracováním osobních údajů musí být stejně snadné jako souhlas poskytnout.

S ohledem na skutečnost, že problematika ochrany osobních údajů je značně komplexní, představují shora uvedené informace pouze stručné shrnutí. V případě potřeby jakéhokoliv upřesnění nebo doplnění v návaznosti na aktuální vývoj zůstáváme nadále plně k dispozici.

V Praze dne 5.9.2017

Advokátní kancelář Růžha