GDPR – OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Ing. RADKA POLÁKOVÁ

Dne 25. května 2018 nabývá účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Zkratka GDPR vychází z anglického názvu směrnice General Data Protection Regulation.

Vzhledem ke skutečnosti, že v některých jiných státech Evropské unie nebyla ochrana osobních údajů na tak vysoké úrovni jako v České republice a zároveň bylo třeba zohlednit zpracování osobních údajů v celosvětové síti, zejména v komerční sféře na internetu (např. v e-shopech), bylo po mnoha letech diskusí obecné nařízení GDPR v roce 2016 na evropské úrovni přijato.

CO PŘINÁŠÍ NOVÉHO?

GDPR definuje pojmy správce, zpracovatel, pověřenec, příjemce, třetí strana, zvláštní kategorie osobních údajů, subjekt údajů, které byly až na výjimky v určité podobě známy i ze zákona o ochraně osobních údajů.

V GDPR jsou na jedné straně přesněji vymezena práva subjektu údajů (fyzických osob, kterých se osobní údaje týkají) a současně na druhé straně povinnosti správců a zpracovatelů těchto údajů. GDPR také formuluje zásady a principy zpracování osobních údajů. Dále upřesňuje roli Úřadu pro ochranu osobních údajů jako hlavního dozorového orgánu a zvyšuje sazby sankcí za porušení ochrany osobních údajů.

CO VYJADŘUJÍ ZÁSADY GDPR?

Zásady zpracování osobních údajů jsou základními pravidly, od kterých se odvíjejí všechny procesy zpracování a zároveň slouží jako základní podmínky způsobu nakládání s osobními údaji pro správce.

Zásada zákonnosti stanoví, že zpracovávat osobní údaje lze jen na základě jednoho z definovaných právních titulů splnění právní povinnosti, která se na správce vztahuje (právo Unie nebo členského státu) nebo souhlas subjektu údajů.

Zásady korektnosti a transparentnosti ukládají správci povinnost být otevřený ohledně zpracování a zajišťovat co největší míru informovanosti subjektů údajů.

Zásada účelového omezení správci zakazuje – až na výjimky – zpracovávat osobní údaje k jiným účelům, než ke kterým byly shromážděny. Výjimkou z této zásady jsou případy tzv. dalšího zpracování.

Zásada minimalizace údajů určuje, jaké údaje může správce za daným účelem zpracovávat. Zpracovány musejí být vždy pouze takové osobní údaje, které jsou pro dosažení účelu nezbytné, a to pouze v nutném rozsahu.

Zásada přesnosti stanoví, že zpracované osobní údaje musejí být přesné a podle potřeby aktualizované. Správce musí přijmout vhodná opatření k tomu, aby nepřesné osobní údaje vymazal nebo opravil.

Zásada omezení uložení zakotvuje povinnost správce vymazat nebo anonymizovat osobní údaje, které již nepotřebuje pro účel, za kterým byly shromážděny (s výjimkou pro další zpracování).

Zásada integrity a důvěrnosti určuje základní povinnosti při zabezpečení zpracování osobních údajů správcem. Správce musí přijmout vhodná technická a organizační opatření, aby zajistil integritu a důvěrnost osobních údajů.

Zásada odpovědnosti ukládá správci povinnost zajistit soulad se všemi výše uvedenými zásadami a být schopen tento soulad prokázat. Pro dodržení této povinnosti bude správce muset uchovávat důkazy ohledně všech opatření, která přijal s cílem zajistit soulad s GDPR, jako jsou dokumentace systémů zpracování, popisy bezpečnostních opatření, důkazy o splnění informační povinnosti nebo udělených souhlasech se zpracováním.

JAKÁ JSOU NOVÁ PRÁVA SUBJEKTU ÚDAJŮ?

- Právo na informace o zpracování osobních údajů.
- Právo na přístup k osobním údajům.
- Právo na opravu.
- Právo na omezení zpracování.
- Právo vznést námitku.
- Právo nebýt předmětem automatizovaného rozhodnutí.
- Právo na výmaz, neboli „právo být zapomenut“, které se neuplatňuje u údajů nezbytných pro výkon veřejné moci.
- Právo na přenositelnost údajů, které se neuplatňuje u údajů nezbytných pro výkon veřejné moci.

JAKÉ POVINNOSTI MÁ SPRÁVCE?

- Posoudit rizikovost zpracování osobních údajů a případně přijmout dodatečná technická a organizační opatření pro záměrnou a standardní ochranu osobních údajů.
- Popsat jednotlivá zpracování, včetně využití informačního systému a ověřit, zda je plněn účel zpracování k doložení, že jsou údaje zpracovávány v souladu s GDPR.
- Vytvořit záznamy o činnostech zpracování, tj. popsat kategorie subjektu údajů a osobních údajů, příjemce a předávání do třetích zemí, případně obecný popis technických a organizačních opatření.
- Upřesnit smluvní vztahy se zpracovateli u stávajících smluv i ve vyhlašovaných výběrových řízeních tzv. zpracovatelskou doložkou.
- Jmenovat pověřence pro ochranu osobních údajů a sdělit jeho kontaktní údaje dozorovému úřadu, tj. Úřadu pro ochranu osobních údajů.
- Zabezpečit práva subjektu údajů.
- Zajistit proces vyřizování žádostí subjektů údajů podle GDPR.
- Zajistit proces ohlašování narušení zabezpečení ochrany osobních údajů Úřadu pro ochranu osobních údajů, případně subjektům údajů.
- Proškolit zaměstnance.
- U připravovaných zpracování provést posouzení vlivu na ochranu osobních údajů.

Výše uvedený postup je nutné přizpůsobit právnímu postavení správce a dále pravidelně a průběžně hodnotit a aktualizovat, tj. nastavit frekvenci auditu a pravidla aktualizace.

CO JE ZÁMĚRNÁ A STANDARDNÍ OCHRANA?

Záměrná ochrana (protection by design): S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jejichž účelem je provádět zásady ochrany údajů a zajistit nezbytné záruky při zpracování osobních údajů, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů. Takovými opatřeními jsou např. anonymizace, pseudonymizace nebo minimalizace údajů.

Standardní ochrana (protection by default): Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje byly standardně zpřístupněny pouze oprávněným fyzickým osobám.

ZÁVĚREM

Pro organizaci, jakou je ČSSZ, která již v současnosti dodržuje zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, a která v právním postavení správce kritické informační infrastruktury Integrovaného informačního systému ČSSZ zavádí a provádí bezpečnostní opatření podle právních předpisů upravujících zajištění kybernetické bezpečnosti, **neznamená GDPR zásadní změnu ve zpracování osobních údajů**. ■

Autorka článku pracuje v oddělení metodiky správy dat ČSSZ.

ZEMŘEL PROFESOR IGOR TOMEŠ

Dne 23. března 2018 zemřel v nedožitých 87 letech **prof. JUDr. Igor Tomeš, CSc.**, odborník působící v oblasti sociální politiky, práva sociálního zabezpečení a sociální správy a dlouholetý spolupracovník redakce Národního pojištění. Vystudoval Právnickou fakultu Univerzity Karlovy v Praze, kde absolvoval také externí aspiranturu a později zde byl jmenován docentem a nakonec profesorem. Profesně působil v Mezinárodní organizaci práce v Ženevě, na Právnické fakultě Univerzity Karlovy a po nuceném odchodu z fakulty v Technicko-ekonomickém ústavu hutního průmyslu. Po roce 1989 působil na Ministerstvu práce a sociálních věcí jako první náměstek ministra a vrátil se také ke své pedagogické činnosti na několika vysokých školách. V roce 1992 založil katedru sociální práce na Filozofické fakultě Univerzity Karlovy v Praze.

Pro Národní pojištění vytvořil v letech 2014–2016 sérii článků, shrnutých do publikace 90 let sociálního pojištění v České republice, a další zajímavé stati.