GDPR v praxi personalisty

JUDr. Jaroslav Stránský, Ph.D.

12. 12. 2017

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Na Březince 14, Praha 5,
tel: +420 251 550 576, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Obecné nařízení o ochraně osobních údajů

- 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 (obecné nařízení o ochraně osobních údajů) vstoupí v účinnost dne 22. května 2018.
- Jde o nařízení, nikoli směrnici.
- Nařízení je přímo použitelné (podobně jako zákon).
- V návaznosti na přijetí Nařízení dojde k:
  - nahrazení dosavadního zákona č. 101/2000 Sb., o ochraně osobních údajů (ZOOU) novým zákonem o zpracování osobních údajů, nebo
  - novelizaci stávajícího zákona.

Obecné nařízení o ochraně osobních údajů

- Existující informace a doplňující materiály k Nařízení:
  - základní příručka k GDPR na www.uoou.cz
  - desatero omylů o GDPR na www.uoou.cz
  - výkladová stanoviska WP 29 (odkazy na www.uoou.cz)
  - Výkladové materiály Evropské komise (dostupné na http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404)
- Očekává se vydání dalších výkladových a prováděcích materiálů ze strany Evropské komise i WP 29.

Základní informace

- Nařízení nepředstavuje zásadní přelom v přístupu k ochraně osobních údajů.
- Přináší některé nové povinnosti a pravidla, prohlubuje ochranu osobních údajů, poskytuje subjektům nová práva.
- Ideově i terminologicky nicméně navazuje na dosavadní směrnici i ZOOU.
- Správci, kteří dosud postupují v souladu s ZOOU splňují i většinu povinností podle Nařízení.

Základní pojmy

- Osobní údaje: 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.
- Zvláštní kategorie osobních údajů (dříve citlivé údaje): údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Základní pojmy

- Zpracování: jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn pomocí či bez pomoci automatizovaných postupů. Jde například o shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, síření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
- Správce: kdokoli, kdo určuje účely a prostředky zpracování osobních údajů.
- Zpracovatel: ten, kdo provádí zpracování pro správce.

Zásady zpracování osobních údajů

- Zákonnost, korektnost a transparentnost. Zákonnost znamená, že pro zpracování existuje některý z důvodů (titulů) upravených Nařízením.
- Účelové omezení (osobní údaje smějí být shromažďovány jen pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný). Každý zpracovatel tedy vždy musí určit účel zpracování osobních údajů.
- Minimalizace (zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány).

Zásady zpracování osobních údajů

- Přesnost (osobní údaje musí být přesné a v případě potřeby aktualizované),
- Omezení uložení (osobní údaje musí být uloženy ve formě umožňující identifikace subjektu údajů jen po dobu, která je nezbytná pro účely, pro něž jsou osobní údaje zpracovávány),
- Integrita a důvěrnost (osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodou ztrátou, zničením nebo poškozením).

Právní titul zpracování

- Podmínkou zákonnosti je existence právního titulu pro zpracování.
- ZOOU uvádí jako hlavní právní titul souhlas a následně uvádí výjimky, kdy souhlas pro zpracování není potřeba.
- Nařízení uvádí výčet rovnocenných právních titulů:
  - souhlas,
  - plnění smlouvy, jejíž stranou je subjekt, nebo provádění opatření před uzavřením smlouvy na žádost subjektu,
  - plnění právní povinnosti správce,
  - ochrana životně důležitých zájmů subjektu nebo jiné fyzické osoby,
  - splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
  - nezbytnost pro účely oprávněných zájmů správce či třetí strany, pokud před těmito zájmy nemají přednost zájmy subjektu, zejména jde-li o dítě.

Souhlas se zpracováním

- Souhlas musí být svobodný a informovaný.
- Subjekt musí vědět:
  - k jakému zpracování jakého údaje dává souhlas,
  - za jakým účelem zpracování probíhá,
  - na jakou dobu souhlas dává.
- Souhlas musí být jasně odlišitelný od případných jiných skutečností. Uzavření jiné smlouvy nemůže být podmíněno souhlasem se zpracováním osobního údaje.
- Správce musí být schopen doložit, že subjekt údajů udělil souhlas se zpracováním.
- Subjekt má právo souhlas kdykoli odvolat.

Nadbytečné vyžadování souhlasu

- Není správné a souladné s právní úpravou vyžadovat souhlas subjektu tam, kde existuje jiný právní titul pro zpracování.
- Nadbytečné vyžadování souhlasu představuje klamání subjektu (myslí si, že údaj je zpracováván na základě souhlasu, ačkoli ve skutečnosti je zpracováván z jiného důvodu).
- V případě nadbytečného udělení souhlasu hrozí riziko nejasností v případě odvolání souhlasu subjektem.
- Správce má vyžadovat souhlas tehdy, když pro zpracování nemá jiný právní titul.

Zpracování na základě souhlasu

- I v pracovněprávních vztazích musí někdy zaměstnavatel získat souhlas zaměstnance se zpracováním osobních údajů.
- Například jde o:
  - fotografie za účelem prezentace zaměstnanců na webových stránkách společnosti,
  - údaje, které zaměstnavatel předává v rámci koncernu, typicky mateřské společnosti,
  - údaje předávané finanční instituci, která zaměstnancům na základě zprostředkování zaměstnavatelem poskytuje finanční produkt (například pojištění pro případ povinnosti k náhradě škody).

Zpracování pro plnění právní povinnosti

- Jde o časté případy, kdy správce zpracovává osobní údaje nikoli proto, že sám chce, nýbrž proto, aby dodržel právní povinnost uloženou:
  - právem EU nebo
  - právem členského státu.
- Zaměstnavatel jako správce typicky zpracovává o svých zaměstnancích za účelem splnění povinností údaje o:
  - rodném čísle a datu narození,
  - počtu vyživovaných dětí,
  - zdravotní pojišťovně,
  - čísle bankovního účtu,
  - doručovací adrese,
  - vzdělání a kvalifikaci atd.

Zpracování pro plnění právní povinnosti

- Zaměstnavatel má také právní povinnost spočítat a zaplatit zaměstnanci mzdu.
- Pokud zpracováním mezd zaměstnavatel pověří třetí osobu, stále jde o zpracování na základě právní povinnosti.
- Zaměstnanec nemusí udělovat souhlas s předáním třetí osobě, ale musí být o tomto zpracování údajů informován.
- Smlouva uzavřená mezi zaměstnavatelem a třetí osobou musí pamatovat i ochranu a zabezpečení osobních údajů zaměstnanců.

Plnění nebo uzavírání smlouvy

- Zpracování v souvislosti s uzavíráním smlouvy probíhá typicky v rámci obsazování nových pracovních pozic.
- Zaměstnavatel tedy nepotřebuje souhlas ke zpracování informací obsažených v životopisu uchazeče o zaměstnání.
- Pokud by si ovšem zaměstnavatel chtěl ponechat životopis (spíše jen kontaktní údaje) neúspěšného uchazeče, šlo by o zpracování na základě souhlasu.
- Plnění smlouvy, případně ochrana oprávněných zájmů představuje zpravidla důvod pro zpracování údajů, které tvoří standardní obsah osobního spisu zaměstnance.

Účel zpracování

- Účel zpracování osobních údajů musí být:
  - určitý,
  - výslovně vyjádřený,
  - legitimní.
- Stanovení účelu zpracování osobních údajů musí předcházet samotnému shromažďování a zpracování osobních údajů.
- Subjekt musí být o účelu zpracování informován.
- Osobní údaje mohou být zpracovávány jen za tímto stanoveným účelem.

Pověřenec pro ochranu osobních údajů

- V originálním znění Data Protection Officer.
- Správce musí jmenovat pověřence v případě, kdy:
  - zpracování provádí orgán veřejné moci či veřejný subjekt,
  - hlavní činnost správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
  - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů podle čl. 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10.
- Pověřenec může být společný pro několik správců.

Pověřenec pro ochranu osobních údajů

- Pověřenec:
  - musí mít profesní a odborné kvality, nevyžaduje se ovšem žádná certifikace či přezkoušení,
  - může být zaměstnancem, ale také nemusí,
  - musí být nezávislý, je vázán mlčenlivostí,
  - nesmí být ve střetu zájmů.
- Pověřenec má:
  - být zapojen do všech záležitostí souvisejících s ochranou osobních údajů,
  - pomáhat při zajišťování souladu zpracování se Nařízením,
  - sledovat průběh zpracování osobních údajů, upozorňovat na nesrovnalosti,
  - poskytovat správci informace a poradenství.
- Pověřenec nemůže dostávat pokyny týkající se výkonu uvedených úkolů.

Povinnost vést záznamy

- Správce je povinen vést záznamy o činnostech zpracování, za něž odpovídá.
- Záznamy musí obsahovat:
  - jméno a kontaktní údaje správce, případně zástupce správce a pověřence,
  - účely zpracování,
  - popis kategorií subjektů údajů a kategorií osobních údajů,
  - kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny,
  - informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci,
  - plánované lhůty pro výmaz údajů, je-li to možné,
  - obecný popis technických a bezpečnostních opatření k zabezpečení osobních údajů, je-li to možné.
- Povinnost vést záznamy se nevztahuje na podnik nebo organizaci zaměstnávající méně než 250 osob.

Nová oprávnění subjektů

- Nařízeno rozšířilo práva subjektů osobních údajů.
- Základní práva subjektu:
  - být informován o zpracování,
  - přístup k osobním údajům,
  - na opravu,
  - na výmaz (právo být zapomenut),
  - na přenositelnost,
  - na omezení zpracování,
  - vznést námitku.

Transparentnost, přístup k údajům

- Všechny informace o ochraně osobních údajů určené subjektu údajů byly stručné, snadno přístupné a srozumitelné.
- Informace lze poskytnout písemně i jinými prostředky.
- Správce má nastavit mechanismy pro podávání žádostí, případně zajištění přístupu k osobním údajům, jejich opravy nebo výmaz, případně postup pro uplatnění práva vznést námitku.
- V souvislosti se vstupem Nařízení v účinnost lze doporučit informovat subjekty údajů o rozsahu zpracovávaných údajů, způsobu zpracování i o jejich právech.

Informace při sběru údajů

- Pokud se osobní údaje týkající se subjektu získávají přímo od subjektu, má správce povinnost v okamžiku získání osobních údajů poskytnout informace:
  - totožnost a kontaktní údaje správce a jeho případného zástupce,
  - kontaktní údaje pověřence,
  - účely zpracování a právní základ pro zpracování,
  - oprávněné zájmy správce nebo třetí strany, dochází-li ke zpracován na základě tohoto důvodu,
  - příjemce nebo kategorie příjemců osobních údajů.

Odpovědnost správce

- S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.
- 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, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.

Odpovědnost správce

- 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 nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

Zabezpečení osobních údajů

- 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, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
  - pseudonymizace a šifrování osobních údajů,
  - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
  - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,
  - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Zabezpečení osobních údajů

- Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
  - náhodné nebo protiprávní zničení,
  - ztráta,
  - pozměňování,
  - neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo
  - neoprávněný přístup k nim.
- Způsob a prostředky zabezpečení ochrany osobních údajů musí správce zdokumentovat.
- Jde o jednu ze záležitostí, která by měla být upravena ve vnitřní řídícím dokumentu (vnitřním předpisu) o zpracování a ochraně osobních údajů.

Ohlašování případů porušení zabezpečení osobních údajů

- Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
- Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.

Dozorový orgán, kontroly a pokuty

- Dozorovým orgánem zůstává Úřad pro ochranu osobních údajů.
- Úřad mimo jiné může provádět kontroly. Při zjištěním porušení může uložit vhodná opatření, případně i uložit pokutu.
- Uložení pokuty musí být v každém jednotlivém případě:
  - účinné,
  - přiměřené a
  - odrazující.

Rekapitulace, úkoly související s Nařízením

- Zjistit, jaké osobní údaje jakých subjektů jsou zpracovávány.
- Ověřit, zda jsou všechny osobní údaje zpracovávány za určitým legitimním účelem.
- Ukončit zpracovávání zbytečných údajů.
- Ověřit, zda jsou údaje zpracovávány na základě souhlasu, nebo bez něj.
- V případě zpracovávání na základě souhlasu zjistit, zda byl udělen a zda byl udělen v souladu s podmínkami Nařízení.
- Zjistit, zda je třena jmenovat pověřence a případně jej jmenovat.
- Zkontrolovat smlouvy se třetími osobami
- Kontrola opatření k zabezpečení osobních údajů a jejich dokumentace.

Děkuji za pozornost!

Tento webinář 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
www.forum-media.sk