

V Praze, dne 25.5.2018

Vnitřní nařízení zaměstnavatele č. 1/2018

Společnost: Traveller sro
IČO: 00676942
DIČ: CZ00676942
se sídlem: Přemyslovská 4, 130 00 Praha 3
zastoupený: Markéta Rohrwasserová
(dále jen správce)

General Data Protection Regulation (GDPR)

Nařízení pro aplikaci a řízení ochrany osobních údajů vnitřním předpisem

Účinnost: od 25.5.2018

Schválil: Markéta Rohrwasserová

Obsah:

- I. Úvod, účel nařízení, prameny právní úpravy ochrany osobních údajů
- II. Základní pojmy
- III. Režimy zpracování osobních údajů správcem
- IV. Výstupy z auditu, další opatření
- V. GDPR pověřenec
- VI. Záznamy o činnostech zpracování
- VII. Závěr

I.

Úvod, účel nařízení, prameny právní úpravy ochrany osobních údajů

Dne 25. 5. 2018 nabyde 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 (**obecné nařízení o ochraně osobních údajů**), dále již jen „GDPR“.

GDPR bude účinné i v České republice, a to z povahy nařízení přímo, aniž by bylo nutné vydávat český speciální zákon, jehož přijetí lze ovšem očekávat.

GDPR nebude jediným právem práva v oblasti ochrany osobních údajů, těmi jsou zejména následující účinné české právní předpisy:

- zák. č. 101/2000Sb. o ochraně osobních údajů a o změně některých zákonů
- zák. č. 89/2012 Sb. občanský zákoník (ochrana osobnosti, satisfakční nároky...)
- zák. č. 40/2009 Sb., trestní zákoník

Jako pomůcka při implementaci GDPR do firemní praxe dobře poslouží i metodické pokyny a doporučení, např. Úřadu na ochranu osobních údajů - viz www.uoou.cz, MV ČR - viz www.mvcr.cz a MŠMT ČR - viz www.msmt.cz (řeší např. téma pověřence pro ochranu osobních údajů).

II.

Základní pojmy

Osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Citlivým osobním údajem se rozumí osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

Anonymní údajem se rozumí takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují.

Zpracování osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

Správce je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.

Zpracovatel každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

Souhlas subjektu údajů je svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.

III.

Režimy zpracování osobních údajů správcem

1. Zpracování bez souhlasu subjektu údajů:

Naprostou většinu osobních údajů uvnitř firmy zpracovávají pověřený a proškolený zaměstnanci na základě zákonného příkazu či přivolení (viz např. zákoník práce, právní předpisy v oblasti zdravotního a sociálního pojištění, pro účely archivnictví apod.). Zpracování je v těchto případech **nezbytné pro splnění zákonných povinností správce**. Dále do této kategorie spadají případy, kdy je zpracování nezbytné pro ochranu práv a právem chráněných zájmů správce a subjektů údajů - sem zahrnujeme např. evidenci návštěv či kamerový monitoring.

Je přípustné pořídít též záznam o pracovním úrazu zaměstnance, např. formou fotografie či videa.

V podmínkách se jedná mj. o záznamy z pracovních porad, knihy úrazů, záznamy o pracovních úrazech, lékařské posudky, personální, mzdovou evidenci, evidenci účetní apod.

Souhlasu zaměstnance není třeba k jeho prezentaci na webu společnosti, zveřejněny však mohou být pouze informace o jeho jménu, titulu, funkčním zařazení, firemních kontaktech.

2. Zpracování se souhlasem subjektu údajů

Pokud nebude dána žádná zákonná povinnost či možnost popsaná v této směrnici, je zcela nezbytné vyžadovat souhlas subjektu údajů, a to z důvodu opatrnosti v písemné formě.

Souhlas musí být:

Svobodný, srozumitelný, doložitelný po celou dobu zpracování osobních údajů a kdykoliv v budoucnu odvolatelný.

Vzorový souhlas:

„Souhlasím po dobu trvání mého pracovního poměru ve společnosti Traveller sro . s pořízením a zveřejněním mých fotografií pořízených během akcí typu konference, školení, teambuilding na webových stránkách firmy. Tento souhlas může být kdykoliv odvolán písemným prohlášením doručeným jednateli - společníkům“.

IV. Další opatření

Vhodná technická, personální a organizační opatření s cílem zajistit a doložit kontrolním orgánům, že osobní údaje zpracováváme v souladu s GDPR a org. směrnicí „Zajišťování personální práce“.

Objektová bezpečnost: zabezpečení firemních objektů a místností, uložení dokumentací, vynášení dokumentací s osobními údaji mimo firmu, analýza rizik neoprávněného či nahodilého přístupu k osobním údajům (kanceláře).

Personální bezpečnost: omezit na minimum okruh zaměstnanců, kteří mají přístup k osobním údajům, prověřit, zda jsou tito zaměstnanci řádně proškoleni v oblasti ochrany osobních údajů, zda jsou doložitelně poučeni o povinnosti mlčenlivosti.

Technická bezpečnost: přístupy do PC, e-maily, hesla, interní a externí úložiště dat, kamerové a docházkové systémy, zabezpečení všech těchto systémů,

Spisový a skartační řád mj. obsahující časovou délku zpracování osobních údajů ve vazbě na tzv. skartační lhůty...“

V. GDPR pověřenec

GDPR příkazuje ustanovit pověřence těm správcům osobních údajů, kteří mají charakter orgánů veřejné moci, veřejným subjektům a zpracovatelům, kteří rozsáhle, pravidelně a systematicky monitorují subjekty údajů.

V naší společnosti se pověřenec **neustanovuje**.

VI. Záznamy o činnostech zpracování

1. Na rozdíl od současného právního stavu účinností GDPR zaniká oznamovací povinnost správce údajů ve vztahu k Úřadu na ochranu osobních údajů - dále jen „ ÚOOÚ“ (např. ohlašování pořízení kamerového systému se záznamem, jeho rozšíření).
2. Nově je správce údajů povinen doložit záznamy o činnostech zpracování **až na výzvu ÚOOÚ**.
3. Obsah záznamu není striktně definován, lze analogicky použít dosud platný registrační formulář z webových stránek ÚOOÚ.

VII. Závěr

V zájmu společnosti je přísné dodržování právní regulace na úseku ochrany osobních údajů. V případě vzniku škody společnosti zaviněním konkrétních zaměstnanců bude tato následně uplatňována postupem stanoveným obecně závaznými právními předpisy.