Směrnice o nakládání s osobními údaji (GDPR)

ÚVOD

Ochrana osobních údajů se stává s rozšířením možností hromadného zpracování a přenosu dat stále důležitější oblastí, neboť s rozvojem informačních technologií roste i riziko zneužití osobních údajů.

V rámci tvorby jednotných pravidel pro celou Evropskou unii byla tato oblast řešena již v minulosti směrnicí 95/46/ES. Vzhledem k rychlému technologickému pokroku však tato směrnice již zastarala.

Dnem 25. května 2018 proto vstupuje v účinnost Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. 4. 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). Nařízení má přímou účinnost, na území ČR ode dne účinnosti stejně jako zákon, dokonce má přednost před vnitrostátním zákonem, takže při rozporu mezi nařízením a zákonem je určující znění nařízení.

Obecné nařízení předpokládá navazující vnitrostátní úpravu zákonem. V ČR však dosud navazující zákon neexistuje. V platném právním řádu je stále zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Tento zákon má řadu ustanovení, která jsou v rozporu s obecným nařízením o ochraně osobních údajů, nařízení má však, jak je uvedeno výše, před zněním tuzemského zákona přednost.

Cílem interních pravidel a postupů je jednoznačně, přehledně a funkčně stanovit pravidla a postupy ochrany osobních údajů, nakládání s osobními údaji, jejich uchovávání, udržování aktuálnosti a odstraňování tak, aby byla vyloučena nebo snížena na přijatelnou minimální úroveň možnost jejich zneužití, úniku nebo neoprávněnému nakládání s nimi.

V dalším textu se používá termín správce osobních údajů a zpracovatel osobních údajů, vyjadřuje se tím organizace/zaměstnavatel, resp. ti její zaměstnanci či představitelé, kteří získání, uchovávání nebo zpracování osobních údajů provádějí, řídí, kontrolují či mají k těmto údajům přístup.

Tento souhrn interních pravidel byl zpracován na základě aktuálně platné legislativy a s přihlédnutím k převažujícímu (obvyklému) výkladu, po posouzení rizik spojených se získáváním uchováváním a zpracováním osobních údajů, a to s vynaložením přiměřené odborné péče tak, aby vyjadřoval zásady záměrné a standardní ochrany osobních údajů.

OSOBNÍ ÚDAJE

Osobní údaje jsou základní údaje o žijící fyzické osobě, a to bez ohledu na to, zda je tato osoba podnikající či nikoli. Osobním údajem se tedy typicky rozumí údaje identifikující fyzickou osobu v postavení zaměstnance, zájemce o zaměstnání, bývalého zaměstnance, obchodního partnera, bývalého obchodního partnera, zájemce o obchodní vztah atd.

Za osobní údaje se nepovažují údaje o zemřelých osobách a anonymizované údaje. Osobními údaji též nejsou údaje o právnických osobách.

Osobním údajem je především jméno, příjmení, pohlaví, věk, datum narození, rodné číslo, osobní stav, občanství, fotografie, bydliště, ale i jakékoli další údaje identifikující dotyčnou osobu jako telefonní číslo, e-mailová adresa, adresa zaměstnání nebo jiné ověřovací identifikační údaje.

Dále je zavedena kategorie citlivých údajů, které je možné zpracovávat jen výjimečně, při dodržení zvláštních omezení, jako rasový nebo etnický původ, náboženské vyznání, politické názory, sexuální orientace, údaje o zdravotním stavu, členství v odborech, údaje o trestních deliktech, osobní údaje dětí (nezbytný je souhlas rodiče), genetické a biometrické údaje atd.

Osobní údaje mohou být zpracovávány jen ze zákonných důvodů a zákonem stanoveným způsobem. Není-li pro uchovávání nebo zpracování osobních údajů zákonný důvod, je nezbytný souhlas osoby, o jejíž osobní údaje se jedná.

Odpovědnost za ochranu osobních údajů:

Výkonný ředitel spolku TOPAZ

ZÍSKÁVÁNÍ OSOBNÍCH ÚDAJŮ

Správce údajů, zapsaný spolek TOPAZ získává osobní údaje o 2 základních okruzích fyzických osob, a to o zaměstnancích a o obchodních partnerech/účastnících/klientech (dále jen klientech).

Údaje o zaměstnancích jsou získávány při vstupu zaměstnance do zaměstnání (získání osobních dat nezbytných pro splnění povinností ukládaných státem formou zákonů při odvodu daní a zákonného pojištění). Tyto údaje jsou průběžně aktualizovány při každé objektivní změně osobního údaje, a to nahlášením ze strany zaměstnance. Při ukončení pracovně-právního vztahu musí být všechny osobní údaje zaměstnance vymazány s výjimkou těch, která je zaměstnavatel po dobu stanovenou zákonem povinen uchovávat

(zejména pro účely daňové kontroly, kontroly správy sociálního zabezpečení, kontroly zdravotní pojišťovny).

Údaje o klientech jsou získávány při uzavírání smluvního vztahu, ať již k němu dochází písemně nebo ústně. Tyto údaje zahrnují údaje o všech fyzických osobách, ať už v postavení zaměstnance, zaměstnavatele, pověřené osoby a podobně. Ke zpracování osobních údajů poskytnutých v souvislosti s obchodním vztahem není třeba zvláštní souhlas. Pokud však jsou osobní údaje uchovávány po skončení smluvního vztahu nad rámec zákonných povinností (např. po lhůtě pro případné provedení daňové kontroly), je nutný souhlas dotyčné fyzické osoby, ten musí být jasně formulován s uvedením identifikace správce získaných údajů a účelu, pro který se údaje získávají. Souhlas nesmí být vysloven předem zaškrtnutým políčkem v internetovém či listinném formuláři. Stejně tak je třeba souhlasu dotyčné osoby při uchovávání či zpracování jejích osobních údajů pro další oslovení např. zasláním newsletteru nebo jiného informačního sdělení. Takové souhlasy jsou získávány v listinné i digitální podobě.

Při získání osobních údajů z jiného zdroje než od dotyčné fyzické osoby je TOPAZ, z.s., povinnen dotyčnou fyzickou osobu informovat o získání jejích osobních údajů a o tom, k čemu budou osobní údaje využity.

Při předávání osobních údajů jiné právnické nebo fyzické osobě (např. sdílení klientů v rámci projektů) je nezbytný konkrétní souhlas fyzické osoby, jejíž osobní údaje jsou předávány, s uvedením identifikace těch, kterým jsou osobní údaje předávány, a účelu, pro který se údaje předávají. Je-li toto sdílení nezbytnou podmínkou pro účast fyzické osoby na konkrétní akci (seminář, konference), musí na být na následné sdílení jejích osobních údajů prokazatelně upozorněna. TOPAZ systematicky nezpracovává osobní údaje z fotodokumentace akcí. Účastníci jsou upozorněni na pořízení záznamů a jejich plánované využití.

UCHOVÁVÁNÍ OSOBNÍCH ÚDAJŮ

Osobní údaje jsou uchovávány v listinné podobě v uzamčené schránce v uzamčeném prostoru kanceláří. Přístup k listinným osobním údajům má pouze ředitel, případně zaměstnanci jím písemně pověření k nakládání s příslušnými osobními údaji. Listiny obsahující osobní údaje nesmí být volně přístupné (položené na stole bez přítomnosti osoby, která má k osobním údajům povolený přístup a která odpovídá za to, že osobní údaje neuniknou k nepovolané osobě).

Osobní údaje jsou dále uchovávány v elektronické formě na počítačích, přístup k nim je zabezpečen heslem, které zná jen jednatel, případně osoby, které jsou jednatelem písemně pověřeny k nakládání s příslušnými osobními údaji. Pokud tato osoba nemá bezprostřední kontrolu nad počítačem, musí být od počítače odhlášená.

Data se zásadně nepřenášejí uvnitř subjektu ani vně subjektu prostřednictvím nezašifrovaného přenosu dat (e-mail, skype apod.). Při nutnosti přenosu dat se použije šifrovaný přenos nebo fyzické předání např. na flash paměti.

Směrnice platí i pro externí zpracovatele osobních údajů (externí účetní firma, externí poradenská firma v oblasti marketingu apod.), znalost a přihlášení se k těmto pravidlům a postupům musí být vyjádřeny písemnou formou.

Pokud pomine právní důvod pro uchovávání osobních údajů (souhlas fyzické osoby nebo jiný právní důvod jako plnění smlouvy, trvání pracovně-právního vztahu atd.), je nutné příslušná osobní data, která není povinen správce uchovávat ze zákona, vymazat či zlikvidovat.

Na žádost fyzické osoby je TOPAZ, z.s. povinen její osobní údaje smazat či přestat uchovávat (pokud netrvá povinnosti je uchovávat ze zákonných důvodů). Fyzická osoba má právo na přístup ke svým osobním údajům, na základě její žádosti je tedy subjekt povinen sdělit, jaké osobní údaje o ní uchovává, či potvrdit, že o ní žádné osobní údaje neuchovává. Dále má fyzická osoba právo na opravu chybných osobních údajů o ní uchovávaných. Správce údajů je povinen reagovat na podnět takové fyzické osoby co nejdříve, nejpozději však do 30 dnů. V případě, že její žádosti nevyhoví, je povinen to zdůvodnit. Vždy je však nejprve třeba ověřit totožnost dotyčné fyzické osoby.

Jsou-li osobní údaje fyzické osoby uchovávány pro účely přímého marketingu, měla by být dotyčná fyzická osoba upozorněna na právo kdykoli bezplatně požadovat ukončení uchovávání a zpracování osobních údajů o své osobě. Požadavek na ukončení uchovávání osobních údajů má být proveditelný stejně snadno jako udělení souhlasu, tedy například proklikem v zaslaném newsletteru, jímž se dotyčná osoba odhlásí z odběru a její osobní data se vymažou z distribučního seznamu.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Osobní údaje je možné zpracovávat jen se souhlasem fyzické osoby, o které se osobní údaje zpracovávají, nebo na základě zákonného důvodu pro zpracování osobních údajů.

V případě hromadného zpracování osobních údajů je třeba předem vyhodnotit možná rizika a při vysoké rizikovosti zpracování osobních údajů je nutné zpracovat posouzení dopadů/vlivu zpracování osobních údajů.

TOPAZ, z.s. nemusí vést záznamy o zpracování, neboť je malým nebo středním podnikem, na které se tato povinnost obecně nevztahuje. Pokud by však zpracování osobních údajů probíhalo pravidelně nebo ohrožovalo práva a svobody osob nebo bylo nakládáno s

citlivými údaji či trestními záznamy, musí vést zpracovatel osobních údajů záznamy o činnostech zpracování.

Výše uvedená pravidla platí i při zpracování osobních údajů externím dodavatelem (např. externí účetní), v takovém případě je třeba, aby externí dodavatel byl vázán písemným smluvním vztahem, ve kterém bude specifikován předmět a doba trvání zpracování osobních údajů, povaha a účel zpracování, typ údajů a kategorie osob, jejichž osobní údaje jsou zpracovávány, a riziko pro práva těchto osob. Po dokončení zpracování osobních údajů by měl externí dodavatel dotyčné osobní údaje vrátit nebo smazat, pokud není pro další uchovávání osobních údajů právní důvod.

VZDĚLÁVÁNÍ, KONTROLA A PŘEZKOUMÁNÍ, ÚČINNOST

Všichni zaměstnanci TOPAZ, z.s. musí být prokazatelně proškoleni z pravidel a postupů do 30 dnů od zařazení pravidel a postupů při ochraně osobních údajů do závazných vnitřních předpisů. Zaměstnanci by měli být seznámeni také s tím, že za porušení ochrany osobních údajů je možné uložit zaměstnavateli sankci až do výše 20 mil. eur (cca 500 mil. Kč).

Zaměstnanci jsou povinni dodržovat pravidla a postupy ochrany osobních údajů. Zjistí-li porušení stanovených pravidel a postupů, jsou povinni to jednateli, jenž přijme příslušná nápravná opatření, která odvrátí či minimalizují způsobenou škodu a zajistí, že se pochybení nebude opakovat.

Závažné porušení ochrany dat je správce/zpracovatel osobních údajů povinen nahlásit do 72 hodin Úřadu pro ochranu osobních údajů a fyzické osobě, jíž se porušení pravidel a postupů při nakládání s osobními údaji týká. Ohlášení musí obsahovat popis porušení zabezpečení osobních údajů, jméno odpovědné nebo pověřené osoby, popis důsledků porušení zabezpečení osobních údajů a popis přijatých nápravných opatření.

Vedoucí pracovníci jsou povinni průběžně kontrolovat dodržování stanovených pravidel a postupů při ochraně osobních údajů a svoje poznatky předávat osobě odpovědné za ochranu osobních údajů.

Pravidla a postupy musí podléhat pravidelnému přezkumu, který probíhá nejpozději do 12 měsíců od minulého přezkumu nebo od zavedení pravidel a postupů.

Tato pravidla a postupy nabývají účinnosti dnem 25. 5. 2018, od tohoto data jsou závazná pro všechny zaměstnance TOPAZ, z.s..