Blíží se **revoluce v ochraně osobních údajů**

JUDr. Jiří Žůrek
Úřad pro ochranu osobních údajů

Dne 25. května 2018 vstoupí ochrana osobních údajů při jejich zpracování v evropském prostoru do nové etapy, jelikož **nabude přímé použitelnosti nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů** a o zrušení směrnice 95/46/ES. Po hmotněprávní stránce nahradí současný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, jenž bude nadále upravovat pouze některé procesní aspekty, postavení a organizaci Úřadu pro ochranu osobních údajů, nebo bude v tomto uvedeném rozsahu nahrazen novým zákonem. Seznamte se proto s novinkami, které zmíněné nařízení vnese již brzy do každodenní praxe!

Zmíněná směrnice 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, nezabránila roztříštěnosti právní úpravy v jednotlivých členských státech, přesněji řečeno si konkrétní země Evropské unie postupem času začaly jednotlivé prováděcí právní předpisy upravovat podle svých představ. De facto tak opět vznikla nejednotnost právního rámce ochrany osobních údajů v evropském prostoru.

Proto – a také a s ohledem na nezbytnost reagovat na postupující digitalizaci života, převažující automatizaci zpracování osobních údajů a jejich celosvětový pohyb a z toho vyplývající nutnost posílit práva subjektů údajů, tj. zpracováním osobních údajů dotčených fyzických osob – bylo nově ke sjednocení právního rámce ochrany osobních údajů v evropském prostoru použito nařízení Evropské unie (dále jen „obecné nařízení"), které se od směrnice EU liší tím, že je přímo použitelné pro jeho adresáty. Správci a subjekty údajů se jím tudíž od výše uvedeného data budou povinni řídit.

Univerzální nařízení

Mezi odbornou veřejností se o obecném nařízení často hovoří jako o revoluci s tím, že se zároveň i zdůrazňují vysoké sankce (dle čl. 83 obecného nařízení lze za některá porušení stanovených povinností uložit pokutu až do výše 20 milionů eur nebo, jde-li o podnik, až do výše 4 % celkového obratu celkového ročního obratu, podle toho, která hodnota je vyšší), jež jsou za porušení obecného nařízení stanoveny. Revoluce je to částečná a to pouze v tom směru, že jde, jak již bylo vysvětleno, o nařízení Evropské unie, které je přímo použitelné a jež se přímo dotkne všech správců se sídlem či provozovnou v EU a zároveň i všech fyzických osob, o nichž budou osobní údaje zpracovávány a které budou, jako subjekty údajů, moci přímo využívat práv stanovených v obecném nařízení.

Právě tato univerzálnost obecného nařízení spočívající jak v aktivním, tak v pasivním dopadu na všechny správce a subjekty údajů v evropském prostoru z něj do jisté míry činí revoluci, jelikož jde o první případ použití toho právního instrumentu v oblasti ochrany osobních údajů.

tip

Pro úplnost je nutné uvést, že se obecné nařízení vztahuje i na zpracování osobních údajů subjektů údajů, jež se nacházejí v Evropské unii, správcem, který v ní není usazen, ale zpracování souvisí s nabídkou zboží či služeb těmto subjektům údajů nebo s monitorováním jejich chování.

Osoba správce a princip odpovědnosti

Z pohledu působnosti obecného nařízení je potřeba zmínit, že subjekt, který je dnes správcem, jím bude i za použitelnosti obecného nařízení. Nemění se ani možnost správce využít pro zpracování osobních údajů zpracovatele, přičemž jsou obecným nařízením stanoveny náležitosti písemné smlouvy mezi ním a zpracovatelem. Obecné nařízení již také výslovně umožňuje tzv. řetězení zpracovatelů, a to za podmínky předchozího písemného povolení správce.

Jelikož je právo na ochranu osobních údajů jedním ze základních práv, jemuž jsou imanentní určité zásady, které byly součástí směrnice 95/46/ES a zákona o ochraně osobních údajů a jež jsou samozřejmě obsaženy v obecném nařízení, nemůže ani v tomto ohledu být obecné nařízení revolucí. Mezi tyto zásady, na kterých je celá ochrana osobních údajů založena a od nichž se odvíjejí i další povinnosti správce, patří zákonnost, korektnost, transparentnost, omezení účelu (v obecném nařízení nešťastně přeloženo jako „účelové omezení"), minimalizace, přesnost a zabezpečení osobních údajů. Za dodržení těchto zásad, které jsou výslovně uvedeny v čl. 5 obecného nařízení, odpovídá správce osobních údajů, navíc musí být schopen jejich dodržení doložit. Jde o tzv. princip odpovědnosti.

Právní důvody umožňující zpracování osobních údajů

Aby bylo jakékoliv zpracování osobních údajů vůbec možné považovat za legitimní neboli zákonné, musí správce disponovat tzv. právním důvodem, který jej opravňuje ke zpracování osobních údajů. Jinými slovy, jde o právem předvídanou dovolenou možnost s osobními údaji disponovat (zpracovávat je). Právní důvod se odvozuje od účelu, pro který správce osobní údaje zpracovává. Účel zpracování osobních údajů, jenž nesmí být v rozporu s právním řádem, může být stanoven vlastním rozhodnutím správce nebo může vyplývat – ať už přímo, či nepřímo – z právních předpisů nebo může být nedílnou součástí nějakého jednání (např. uzavírání smlouvy s fyzickou osobou).

Splnění zásady zákonnosti je tak vůbec prvním a nezbytným předpokladem, aby mohlo být zpracování osobních údajů označeno jako souladné s obecným nařízením, jelikož pokud by správce nedisponoval řádným právním důvodem pro zpracování osobních údajů, měl by je nezákonně a již by nebylo rozhodné a ani omlouvající, že by řádně plnil některé jiné povinnosti kladené obecným nařízením.

Zpracování osobních údajů bez souhlasu subjektu

Rozeznáváme dvě skupiny právních důvodů umožňujících zpracování osobních údajů. První skupinu tvoří právní důvody, které opravňují správce zpracovávat osobní údaje bez souhlasu subjektu údajů. Do této skupiny obecné nařízení řadí zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro účely jejího uzavření, zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje, zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, zpracování nezbytné pro účely oprávněných zájmů správce či

třetí strany a konečně zpracování, které je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Všechny tyto vyjmenované právní důvody jsou de facto obsaženy i v zákoně o ochraně osobních údajů. V rámci této skupiny se nejčastěji v praxi využívá pro zpracování osobních údajů právní důvod „účely plnění smlouvy" či „plnění zákonem stanovené povinnosti". V praxi je též časté využití právního důvodu umožňujícího zpracovávat osobní údaje, pokud je to nezbytné pro účely oprávněných zájmů správce [tento právní důvod je často využíván pro kamerové systémy využívané pro ochranu oprávněných zájmů správce (majetek) a třetích osob (život a zdraví)].

Obecné nařízení oproti zákonu o ochraně osobních údajů výslovně neuvádí jako právní důvod umožňující dále zpracovávat osobní údaje oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem ani možnost poskytovat osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním či pracovním zařazení. Druhý jmenovaný právní důvod však úzce souvisí s právem na informace, a tudíž lze očekávat, že tyto informace nadále budou veřejnosti poskytovány, například na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Souhlas se zpracováním osobních údajů

Druhou skupinu tvoří jediný právní důvod, a to souhlas se zpracováním osobních údajů. Obecné nařízení nově explicitně stanovuje podmínky vyjádření souhlasu a za zmínku stojí nutnost zajistit odlišitelnost souhlasu od jiných skutečností při uzavírání písemné smlouvy, tzn. že (automaticky presumovaný) souhlas již nesmí být přímo součástí smlouvy nebo součástí obchodních podmínek, ledaže by forma smlouvy či obchodních podmínek umožňovala souhlas neudělit.

Půjde tak o změnu oproti současné situaci, kdy mnoho správců, respektive obchodních společností, používá tzv. formulářové smlouvy (tj. smlouvy typu „ber, nebo nech být", kdy zákazník nemá možnost vyjednávat o změnách) a zároveň je v ustanovení smlouvy či obchodních podmínkách, jež tvoří nedílnou součást uzavírané smlouvy, obsažen již předem presumovaný souhlas zákazníka (subjektu údajů) se zpracováním osobních údajů (marketingové účely, předávání v rámci „skupiny podniků" atd.), který není pro účely plnění smlouvy nezbytný. Stanovení podmínky odlišitelnosti souhlasu v obecném nařízení má zabránit tomu, aby se osobní údaje stávaly jakýmsi dalším platidlem, benefitem pro správce, jak je tomu často dnes.

Z povahy souhlasu se zpracováním osobních údajů vyplývá, že jde o svobodný projev vůle, k jehož učinění nemůže být subjekt údajů nucen, což úzce souvisí s nutností odlišit souhlas od hlavního smluvního ujednání. Aby byl souhlas svobodný, musí se zohledňovat i skutečnost, zda je plnění smlouvy podmíněno souhlasem se zpracováním osobních údajů, jež není pro plnění dané smlouvy nutné.

Správci, kteří mají souhlas založen na takto presumovaném, nesvobodném souhlasu, by již v současné době měli provést jeho revizi, zda skutečně ke zpracování osobních údajů potřebují souhlas subjektu údajů, jelikož v praxi se souhlas často vyžaduje i pro zpracování osobních údajů, kterému svědčí právní důvod umožňující osobní údaje zpracovávat bez souhlasu subjektu údajů; pokud správci dospějí k názoru, že je souhlas nezbytný, bude nutné, pokud souhlas nesplňuje mimo jiné shora uvedené náležitosti (tj. odlišitelnost a svobodnost), získat nový. [Viz bod 171 preambule obecného nařízení, který stanovuje následující: Je-li zpracování založeno na souhlasu podle směrnice 95/46/ES (v našich podmínkách myšleno dle zákona o ochraně osobních údajů), není nutné, aby subjekt údajů znovu udělil svůj souhlas, pokud je způsob udělení daného souhlasu v souladu s podmínkami tohoto nařízení.]

Je nutné podotknout, že pokud jsou osobní údaje zpracovávány například za účelem plnění smlouvy a souhlas byl používán pouze pro „nadstavbové" zpracování (zmíněné marketingové účely, předání v rámci „skupiny podniků" atd.), pak neplatný souhlas automaticky neznamená likvidaci osobních údajů, jelikož ty jsou nadále zpracovávány za účelem plnění smlouvy nebo pro plnění zákonem stanovené povinnosti; správce však již nebude moci osobní údaje používat pro účely stanovené v neplatném souhlasu.

Právo na informace o zpracování osobních údajů

Jak je vidět, subjekt údajů musí často strpět zpracování svých osobních údajů, případně má možnost se rozhodnout, že ke zpracování svých osobních údajů svolí. Aby byl tedy vybalancován do jisté míry nevyvážený vztah „správce – subjekt údajů", stanovuje obecné nařízení práva subjektu údajů, a mezi nimi i právo na informace o zpracování osobních údajů, jež má subjektu údajů zajistit informace o zpracování osobních údajů, případně mu poskytnout informace, aby se mohl rozhodnout, zda ke zpracování svých osobních údajů svolí.

Poskytované informace, zejména o totožnosti správce a účelech zpracování, by měly být zřetelné, snadno přístupné a podávané za použití jasných a jednoduchých jazykových prostředků. Jde o projev zásady transparentnosti zpracování osobních údajů. Úplný výčet informací, které by měl správce subjektu údajů poskytnout, nalezneme v čl. 13 a 14 obecného nařízení, přičemž prvně jmenovaný článek se týká informací poskytovaných v případě, že byly osobní údaje získány přímo od subjektu údajů, a druhý se týká informací poskytovaných v případě, že osobní údaje nebyly získány od subjektu údajů.

Zásady omezení účelu a omezení uložení

Osobní údaje musejí být zpracovávány pro výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který by byl s těmito účely neslučitelný. Jde o vyjádření zásady omezení účelu. Správce tak nemůže bezdůvodně rozšiřovat nebo měnit účel zpracovávaných osobních údajů, ledaže by šlo o jejich přiměřené využití pro účely archivace ve veřejném zájmu nebo pro účely vědeckého či historického výzkumu nebo pro statistické účely.

Jelikož každé zpracování osobních údajů může pro subjekt údajů představovat riziko, například v podobě jejich úniku, je vždy vhodné, aby správce zpracovával jen nezbytné minimum osobních údajů, které je potřebné pro naplnění stanoveného účelu. Zároveň, což je promítnutí zásady omezení uložení, by neměl správce uchovávat osobní údaje ve formě umožňující identifikaci po delší dobu, než je nezbytné pro účely, pro něž jsou osobní údaje zpracovávány.

Přesnost a zabezpečení osobních údajů

Zpracovávané osobní údaje by měly být přesné, jelikož zpracování nepřesných osobních údajů postrádá smysl jak pro správce, tak pro subjekt údajů. Obecné nařízení nestanovuje správci aktivní povinnost vyhledávat nepřesné osobní údaje či se periodicky doptávat subjektů údajů, zda se u nich některý z údajů nezměnil; pokud však subjekt údajů požádá o jejich opravu, měl by správce, nemá-li pochybnosti, opravu provést, případně učinit jiná adekvátní opatření.

tip

Přestože je správce povinen osobní údaje zabezpečit, neznamená to – jak lze mnohdy slyšet – automatickou povinnost uchovávat osobní údaje v zašifrované či pseudonymizované podobě. Každý správce si musí zvolit rozumnou míru zabezpečení s ohledem na rozsah a kontext zpracování, přičemž právě šifrování či pseudonymizace mohou být jedním z prvků zabezpečení osobních údajů, zejména pokud jsou zpracovávány zvláštní kategorie osobních údajů (v dnešní terminologii „citlivé osobní údaje").

Poslední zásadou, kterou obecné nařízení přímo vyjmenovává, je zásada integrity a důvěrnosti, což představuje nutnost klást dostatečný důraz na náležité zabezpečení osobních údajů, které se bude odvíjet od rozsahu, kontextu, kategorií zpracovávaných osobních údajů a dalších okolností. Zabezpečení osobních údajů musí být adekvátní s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování.

Kodexy chování a osvědčení

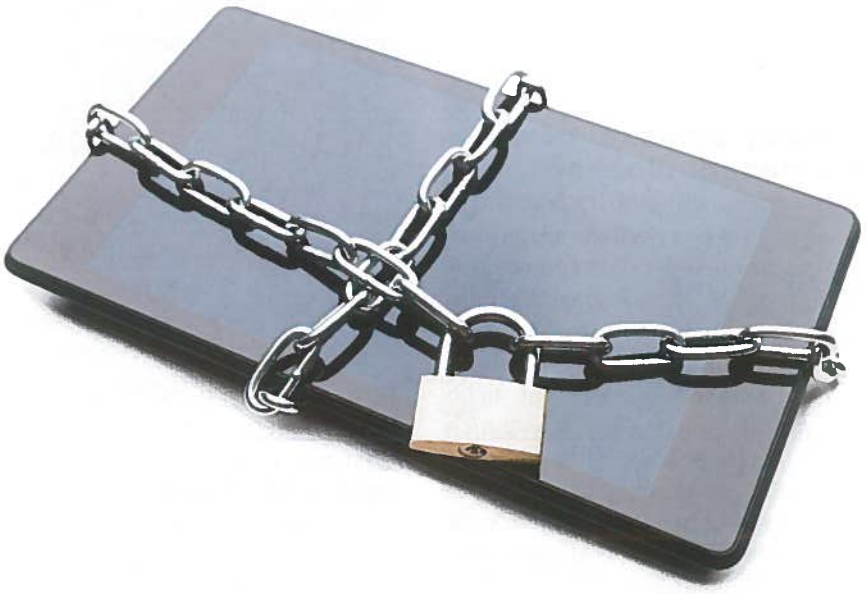
Za plnění shora uvedených zásad správce nejen odpovídá, ale – jak již bylo uvedeno – musí být schopen dodržení souladu s těmito zásadami doložit. Je zřejmé, že každý správce bude v jiném postavení a bude dodržení souladu dokládat jinými způsoby. Obecné nařízení se pokouší správcům ulehčit plnění povinnosti doložit soulad zpracování s obecným nařízením tím, že nově stanovuje možnost vydání tzv. kodexu chování, k jehož dodržování se správce může dobrovolně zavázat, a možnost získat osvědčení.

Kodexy mohou být vypracovávány s ohledem na povahu různých odvětví nebo sektorů. Základem každého kodexu by mohlo být upřesnění oprávněných zájmů, které správci v konkrétních situacích sledují, proces shromažďování osobních údajů, včetně jejich rozsahu, správné formulace poskytovaných informací a další okolnosti zpracování.

V budoucnu se tak bude možné nejspíše dočkat kodexů zpracování osobních údajů pro banky nebo internetové obchody, které budou stanovovat správnou praxi při zpracování osobních údajů v daném odvětví či sektoru. Kodexy budou moci navrhovat a vydávat sdružení nebo jiné subjekty zastupující různé kategorie správců, přičemž dozorový úřad, tedy Úřad pro ochranu osobních údajů, vydá stanovisko, zda je daný návrh kodexu v souladu s obecným nařízením, a pokud ano, schválí jej. Monitorování dodržování kodexu ze strany správce bude moci provádět i subjekt, který bude mít příslušnou úroveň znalostí a bude pro tento účel Úřadem pro ochranu osobních údajů akreditován.

Osvědčení nebo také pečetě či známky by rovněž měly dokládat soulad zpracování s obecným nařízením. Jde o jakýsi audit zpracování nezávislým subjektem, který po posouzení zpracování vydá správci, nejvýše na dobu 3 let (s možností opětovného prodloužení), osvědčení o souladu zpracování osobních údajů s obecným nařízením. Osvědčení bude moci udělovat a obnovovat subjekt s příslušnou úrovní znalostí ohledně ochrany osobních údajů.

Přihlášení se k dodržování vydaného kodexu nebo získání osvědčení tak bude pro správce představovat nejen ulehčení prokazování souladu zpracování se zmíněnými zásadami, ale také zcela nepochybně konkurenční výhodu, vzhledem k narůstajícímu počtu subjektů údajů kladoucích při spotřebitelském rozhodování důraz i na adekvátní ochranu osobních údajů poskytovanou správcem.



Závěrem

Obecné nařízení by ze strany správců nemělo být chápáno jako strašák či jako revoluce, nýbrž coby příležitost pro revizi a audit zpracovatelských operací a nastavení zpracování osobních údajů tak, aby odpovídalo požadavkům obecného nařízení. K tomu ostatně nyní běží dvouletá lhůta, která uplyne k 25. květnu 2018 a během níž je povinností správce uvést zpracování osobních údajů do souladu s obecným nařízením. (Viz bod 171 preambule obecného nařízení, jenž stanovuje následující: Zpracování, které již ke dni použitelnosti tohoto nařízení probíhá, by mělo být uvedeno v soulad s tímto nařízením ve lhůtě 2 let ode dne vstupu tohoto nařízení v platnost. Pozn. autora: Obecné nařízení vstoupilo v platnost 24. května 2016.)

Nové instituty obsažené v obecném nařízení, mezi něž patří například povinnost v některých případech ustavit pověřence pro ochranu osobních údajů, povinnost ohlašovat, respektive oznamovat případy porušení zabezpečení osobních údajů dozorovému úřadu, respektive subjektům údajů, a další nové povinnosti budou popsány v dalším čísle časopisu Statutární zástupce firmy.

Tento článek vyjadřuje pouze osobní názor autora, nikoliv jeho zaměstnavatele.