Květen 2017

Škola ochrany osobních údajů

advokátní kanceláře Balcar, Polanský & Spol. s.r.o.

Nařízení EP a Rady (EU) 2016/679 z 27. dubna 2016, tzv. Všeobecné nařízení o ochraně údajů („Nařízení") zrušilo směrnici 95/46/ES („Směrnice"), která je nyní transformována do českého právního řádu zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Nařízení vstoupí v účinnost dnem 25. května 2018, kdy se stane přímo účinným rovněž v České republice a dotkne se všech, kteří osobní údaje zpracovávají, jakož i fyzických osob, jejichž osobní údaje jsou předmětem zpracování, tedy téměř každého.

Vzhledem k dosud nejvýznamnější legislativní změně evropského rozměru v oblasti ochrany osobních údajů Vám s týdenní frekvencí přinášíme pravidelné informace pro snadnější a efektivnější orientaci v množství povinností, které Nařízení přináší.

Pokud si přejete odebírat Školu osobních údajů přímo do Vaší e-mailové schránky, prosím přihlaste se na adrese office@bapol.cz, popř. na tel. čísle +420 251 009 111.

Lekce 11 z 16

Kodexy chování a vydávání osvědčení

V textu se dozvíte:

Důležité změny

- Nařízení přináší nové instituty k zajištění a prokázání skutečnosti, že zpracování je v souladu s Nařízením, a to:
  - kodexy chování, a
  - mechanismy pro vydávání osvědčení, pečetí nebo známek;
- Prostřednictvím kodexů chování mají správci a zpracovatelé možnost snáze zajistit a dodržovat soulad s Nařízením;
- Dodržování kodexů chování bude monitorováno akreditovanými subjekty; bude-li zjištěno porušení kodexu, může být správce či zpracovatel vyloučen z účasti na kodexu;
- Mechanismy pro vydávání osvědčení, pečetí nebo známek jsou určeny pro dobrovolnou „samoregulaci" správce nebo zpracovatele;
- Bude-li správce nebo zpracovatel disponovat kodexem nebo osvědčením atd., bude to svědčit o souladu s Nařízením, a to po dobu 3 let (platnost osvědčení bude možné prodloužit).

Compliance: Akční plán

Správci a zpracovatelé by měli:

- monitorovat, zda neexistují v jejich odvětví schválené kodexy chování platné v rámci ČR nebo EU;
- zjistit, zda existují mechanismy pro vydávání osvědčení, pečetí nebo známek, které by mohli získat a prokázat tak soulad s Nařízením;
- seznámit se s osvědčeními, pečetěmi nebo známkami, které budou postupně zaváděny, a zohledňovat tyto instituty při výběru svých zpracovatelů nebo subdodavatelů.

Kodexy chování

Nařízení upravuje kodexy chování jako dokumenty, vypracované sdruženími nebo jinými subjekty zastupujícími různé kategorie správců nebo zpracovatelů. Kodexy upravují zpracování osobních údajů specifické pro tyto skupiny správců nebo zpracovatelů. Mají přispět k řádnému uplatňování Nařízení s ohledem na konkrétní povahu různých odvětví a na konkrétní potřeby mikropodniků a malých a středních podniků.

Kodexy tak budou mít význam pro správce a zpracovatele, kteří budou jejich dodržováním jednodušeji a spolehlivě zajišťovat a prokazovat dozorovým úřadům soulad s Nařízením.

To, že se správce nebo zpracovatel zaváže dodržovat schválený kodex chování, může mít několik pozitivních účinků:

- prostřednictvím kodexů budou zavedeny doporučené postupy, jak v daném odvětví a ve specifickém kontextu zpracovávání nakládat s osobními údaji;
- budou se moci spolehnout, že zpracovávání provozují zákonným způsobem, což může ušetřit např. náklady na odborné poradce;
- účast na schváleném kodexu bude u subjektů údajů vzbuzovat důvěru, že jejich údaje jsou zpracovávány zákonným způsobem;
- spolu se závazkem příjemce údajů, sídlícího mimo EU, přijmout vhodné záruky budou kodexy použitelné při zajišťování zákonnosti přenosu údajů mimo EU, podobně jako standardní smluvní doložky a závazná vnitropodniková pravidla; a
- dozorovému úřadu bude snadno prokazatelný soulad s Nařízením.

Sdružení nebo jiný subjekt zastupující různé kategorie správců nebo zpracovatelů může tudíž vypracovat kodex chování relevantní pro daný sektor nebo odvětví. Kodex má sloužit jako „návod" pro společnosti působící v daném odvětví, jak správně zpracovávat osobní údaje pro jejich odvětví specifické, např. subjekty působící v oblasti bankovnictví, zdravotnictví, školství, farmaceutického průmyslu, maloobchodu, IT a cloudových služeb atd.

Kodexy mohou upravovat doporučené postupy například v souvislosti se spravedlivým a transparentním zpracováním, oprávněnými zájmy, jež správci v konkrétních situacích sledují, shromažďováním osobních údajů, pseudonymizací osobních údajů, informacemi poskytovanými veřejnosti a subjektům údajů, výkonem práv subjektů údajů, informacemi poskytovanými dětem a jejich ochraně a způsobem získávání souhlasu nositele rodičovské zodpovědnosti nad dítětem, opatřeními a postupy účelnými pro přijetí vhodných technických a organizačních opatření a specificky navržené a standardní ochrany údajů, opatřeními k zajištění bezpečnosti zpracování, ohlašováním případů porušení zabezpečení osobních údajů dozorovým úřadům a oznamováním těchto případů porušení subjektům údajů, předáváním osobních údajů do třetích zemí nebo mezinárodním organizacím a mimosoudním vyrovnáním a jinými postupy pro řešení sporů mezi správci a subjekty údajů v souvislosti se zpracováním.

Schvalování kodexů

K tomu, aby měl kodex chování vyšší právní účinky, je třeba schválení příslušným dozorovým úřadem. Proces schválení se odvíjí od toho, zda se jedná o kodex s vnitrostátní platností, nebo zda má mít kodex všeobecnou platnost v rámci Unie.

Pokud jde o kodex, který se netýká činností zpracování mimo určitý stát (např. ČR), je třeba jeho návrh předložit příslušnému dozorovému úřadu (v tomto případě Úřadu pro ochranu osobních údajů ČR). Úřad vydá stanovisko, zda je daný návrh kodexu v souladu s Nařízením, a pokud shledá, že poskytuje dostatečné vhodné záruky, návrh schválí. Dozorový úřad také daný kodex zaregistruje a zveřejní.

Jedná-li se naopak o kodex, který se týká činností zpracování v několika členských státech, předloží příslušný dozorový úřad návrh kodexu v rámci spolupráce dozorových úřadů států Unie a Komise Evropskému sboru pro ochranu osobních údajů („Sbor"), který vydá stanovisko, zda je návrh kodexu v souladu s Nařízením nebo zda poskytuje vhodné záruky. Pokud Sbor potvrdí, že návrh kodexu je v souladu s Nařízením či poskytuje vhodné záruky, předloží své stanovisko Komisi. Komise může svým prováděcím aktem rozhodnout, že schválený kodex chování, který jí byl předložen, má všeobecnou platnost v rámci Unie. Komise zajistí odpovídající zveřejnění těchto kodexů s všeobecnou platností. Sbor schválené kodexy chování shromáždí a vhodným způsobem je zpřístupní veřejnosti.

Monitorování dodržování kodexů

Kromě příslušného dozorového úřadu může monitorování souladu s kodexem chování provádět subjekt, který má o předmětu kodexu odpovídající odborné znalosti a je pro tento účel akreditován příslušným dozorovým úřadem. Tento subjekt musí:

- prokázat nezávislost a odborné znalosti o předmětu kodexu;
- stanovit postupy, které mu umožňují posoudit způsobilost dotčených správců a zpracovatelů, pokud jde o uplatňování kodexu, monitorovat, zda jeho ustanovení dodržují, a pravidelně přezkoumávat jeho činnost;
- stanovit postupy a struktury pro řešení stížností na porušování kodexu nebo na způsob, jak správce nebo zpracovatel kodex uplatňoval nebo uplatňuje, a zajistit transparentnost těchto postupů a struktur pro subjekty údajů a pro veřejnost; a
- prokázat, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

Kritéria pro akreditaci určí příslušný dozorový úřad po konzultaci s Evropským sborem pro ochranu osobních údajů. Pokud akreditovaný subjekt zjistí porušení kodexu, může správci nebo zpracovateli uložit sankci v podobě vhodných opatření, včetně pozastavení jejich účasti na kodexu nebo vyloučení z této účasti.

Vydávání osvědčení

Mechanismy pro vydávání osvědčení a zavedení pečetí a známek upravuje Nařízení jako další nové instituty ochrany osobních údajů. Tyto mechanismy mají sloužit zejména k zvýšení transparentnosti zpracování a mají pomoci subjektům údajů při rychlém posouzení úrovně ochrany osobních údajů v případě relevantních produktů a služeb. Jako příklad je možno uvést situaci, kdy se pro určitou službu, např. poskytování cloudových služeb, zavedou pečetě nebo známky, které budou znamenat, že subjekt, který je získá, splňuje požadavky Nařízení pro zákonné zpracování[1].

Vydávání osvědčení pro zpracování osobních údajů je důležitým mezníkem pro vytvoření spolehlivého a transparentního rámce zpracování. Tyto mechanismy mohou být zavedeny

[1] Pro porozumění je možno uvést např. značku ISO, která dokazuje, že subjekt v dané oblasti dosahuje kvalit požadovaných tímto certifikátem.

členskými státy, ale i dozorovými úřady, Sborem či Komisí. Měly by být použitelné především na úrovni Unie, ale není vyloučena ani vnitrostátní platnost. Zohledněny by měly být specifické potřeby mikropodniků a malých a středních podniků.

Vydání osvědčení je dobrovolné, ale nesnižuje odpovědnost správce nebo zpracovatele za soulad s Nařízením. Jinak řečeno, pokud např. správce získá osvědčení, ale navzdory tomu zpracováním poruší Nařízení, osvědčení ho nezbavuje odpovědnosti. Osvědčení se vydává na dobu nejvýše tří let a lze je obnovit za stejných podmínek, pokud jsou i nadále plněny příslušné požadavky. Obdobně, nejsou-li požadavky na osvědčení plněny, může být osvědčení subjektu odebráno.

Osvědčení může mít pro správce a zpracovatele následující výhody:

- správci a zpracovatelé budou moci snáze prokázat soulad s Nařízením, a to především v souvislosti s přijetím vhodných technických a organizačních opatření;
- subjekty údajů, případně zákazníci, kteří se budou rozhodovat pro dodavatele služeb, mohou k osvědčení přihlížet jako k důkazu věrohodnosti a profesionality poskytovatele (např. cloudových) služeb; a
- obdobně jako v případě kodexů, spolu se závazkem příjemce údajů sídlícího mimo EU přijmout vhodné záruky budou osvědčení použitelná při zajišťování zákonnosti přenosu údajů mimo EU, podobně jako standardní smluvní doložky a závazná vnitropodniková pravidla

Nařízení přiznává pravomoc vydávat osvědčení kromě dozorových úřadů také subjektům pro vydávání osvědčení, které získají pro tuto činnost akreditaci. V českých podmínkách bude Úřad pro ochranu osobních údajů oprávněn udělit akreditaci subjektům pro vydávání osvědčení. Pro získání akreditace musí subjekt pro vydávání osvědčení splnit kritéria stanovená Nařízením, mimo jiné:

- prokázat nezávislost a odborné znalosti o předmětu osvědčení;
- zavázat se respektovat kritéria schválená Sborem nebo příslušným dozorovým úřadem;
- stanovit postupy pro vydávání, pravidelný přezkum a odebírání osvědčení, pečetí a známek dokládajících ochranu údajů;
- stanovit postupy a struktury pro řešení stížností týkajících se porušování osvědčení nebo způsobu, jak správce nebo zpracovatel osvědčení uplatňoval nebo uplatňuje, a zajistit transparentnost těchto postupů a struktur pro subjekty údajů a pro veřejnost; a
- doložit, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

Akreditace se vydává na období nejvýše pěti let a lze ji obnovit.

Co dále

Správci a zpracovatelé mohou významně těžit z účasti na schválených kodexech chování (platných vnitrostátně nebo v rámci Unie), nebo z vydávání osvědčení nebo zavedení pečetí a známek, které budou průběžně zaváděny po nabytí účinnosti Nařízení. Z uvedeného důvodu lze doporučit, aby správci a zpracovatelé monitorovali zavádění těchto institutů, aby se mohli včas rozhodnout, zda se jich budou chtít účastnit nebo je získat.

Další informace

Recitály 77, 81, 98 – 100, 148, 166, 168,

Články 40 – 43, 57 odst. 1 písm. p), q), odst. 3 písm. e), 64 odst. 1 písm. c), 70 odst. 1 písm. o), p)

Kontaktní osoba

Pro další informace prosím kontaktujte:

Česká republika:

JUDr. Jaroslav Srb
Advokát

Tel.: +420 220 251 111
Mobil: +420 731 609 510

jaroslav.srb@bapol.cz

Slovensko:

JUDr. Helga Maďarová, CIPP/E
Advokátka | Certified Intl. Privacy Professional/Europe

Tel.: +421 220 251 311
Mobil: +421 917 092 076

helga.madarova@bapol.sk