GDPR: Nejen povinnosti, ale i příležitosti

Stanislav Klika

Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR) nabylo účinnosti 25. 5. 2018. Nařízení změnilo evropskou legislativu v oblasti ochrany osobních údajů. Co to však skutečně znamená pro firmy a organizace v České republice?

Stanislav Klika

V

Obavám ze sankcí se nelze divit. Očekává se totiž, že orgány dohledu budou při prosazování pravidel přísnější.

V ČEM SPOČÍVAJÍ ZMĚNY?

GDPR platí pro všechny subjekty – velké i malé, soukromé i veřejné, firmy i neziskovky. Jedinou podmínkou je, aby firma či organizace zpracovávala osobní údaje občanů Evropské unie.

Nařízení přináší některé nové povinnosti, které mohou nemálo zatížit firemní rozpočty. Mezi tyto povinnosti patří například zavedení role pověřence pro ochranu osobních údajů nebo nové nároky v souvislosti s rozšířením práv lidí na přístup k jejich osobním údajům. Firmy tak musí být například schopny osobní údaje ve svých systémech vyhledat, a pokud o to zákazník požádá, tak musí předat kopie osobních údajů, které o zákaznících zpracovávají. Firmy musí také umět tyto údaje případně smazat. To někdy naráží na informační systémy, které firmy mají. Ty se často vytvářely postupně a jednotlivé verze na sebe nenavazovaly. Aby informační systém zvládl požadavky dané GDPR, bude občas potřeba systém upravit, a to může být velmi nákladné.

Osmdesát procent požadavků GDPR však již dnes obsahuje současný zákon o ochraně osobních údajů nebo tyto požadavky vyplývají z judikatury či stanovisek regulátora. Pro firmy a organizace by tak neměly představovat úplnou novinku. Při našich auditech se však setkáváme s tím, že firmy a organizace nejsou připraveny bohužel ani na plnění stávajících povinností.

Na celou záležitost je tedy možné pohlížet i tak, že ta skutečná změna nespočívá v nových pravidlech (která vycházejí ze stávajících principů), ale v přístupu k plnění těchto norem. Mediální tlak a hrozba vysokých pokut způsobily, že firmy přehodnocují svoje priority a více investují do nastavení procesů zpracování osobních dat v souladu s novou legislativou.

PŘÍSNĚJŠÍ PRAVIDLA HRY

Obavám ze sankcí se nelze divit. Očekává se totiž, že orgány dohledu budou při prosazování pravidel přísnější a jejich porušování může být výhledově také přísněji sankcionováno. Jak je to ale s pokutami nyní? Horní hranice podle stávající právní úpravy činí deset milionů korun pro právnické osoby. Nejvyšší pokuty udělené Úřadem pro ochranu osobních údajů však dosahovaly zhruba poloviny uvedené částky.

GDPR horní hranici možných pokut razantně navyšuje. V případě závažného pochybení může být udělena pokuta až do výše 20 milionů eur nebo v případě podniku až do čtyř procent z celkového ročního světového obratu. Pokutu udělenou v maximální sazbě však nejspíš v České republice hned tak neuvidíme. Důležitým korektivem při ukládání sankcí jsou zásady správního trestání a také právní názor českých soudů, podle kterého nesmí být výše udělené pokuty likvidační.

GDPR A KONKURENCESCHOPNOST

Nové nařízení, či spíše reálná implementace někdy až příliš formalistických zásad ochrany osobních údajů, si vyžádá nemalé finanční náklady na zavedení potřebných opatření i náklady na průběžné dodržování stanovených pravidel. GDPR tak nepřináší ▷

▷ jen lepší postavení subjektů údajů a opatření pro účinnější ochranu soukromí občanů Evropské unie. Evropské požadavky na ochranu osobních údajů nejnověji vyjádřené v GDPR přinášejí i negativa. I když je úmysl evropských orgánů chránit soukromí principiálně správný, evropským firmám vzniknou nové náklady, které rozhodně nejsou zanedbatelné a ve výsledku mohou dlouhodobě navyšovat ceny výrobků a služeb.

Nařízení z hlediska světového obchodu ztíží postavení evropských firem, zejména vůči již dnes velmi levné produkci z Asie.

Dá se tedy předpokládat, že nařízení z hlediska světového obchodu ztíží postavení evropských firem, zejména vůči již dnes velmi levné produkci z Asie, které je velmi těžké konkurovat a kde tak přísná pravidla neplatí. Tomu se snaží Evropská unie čelit zavedením povinností i pro mimoevropské firmy, které například cílí na evropské spotřebitele. Je však těžké si představit vymáhání povinností stanovených GDPR po firmách z druhého konce světa navyklých na zcela jiné standardy a mnohdy i etiku podnikání.

Výši účtu za GDPR ovlivní v prvé řadě úroveň dosavadních firemních procesních a softwarových opatření. Využívá-li firma či jiná organizace kompatibilní software a má-li zavedeny fungující procesy v oblasti ochrany osobních údajů, budou náklady bezvýznamné a půjde spíše jen o formality. Naopak zcela nepřipravená firma, která zanedbala přípravu a s prvními kroky začala teprve na jaře, může zaplatit v důsledku překotných a nepromyšlených změn i statisíce korun navíc.

FORMA NOVÉ PRÁVNÍ ÚPRAVY A ADAPTAČNÍ ZÁKON

Dosavadní právní úprava ochrany osobních údajů vychází ze směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Česká republika implementovala směrnici zákonem č. 101/2000 Sb., o ochraně osobních údajů. GDPR je však nařízení Evropské unie, které má přímé účinky, je závazné přímo pro fyzické a právnické osoby. Není tedy třeba zákona na národní úrovni, díky kterému by se pravidla GDPR uplatnila.

Návrh zákona o zpracování osobních údajů je adaptačním zákonem a má upravovat některé dílčí otázky ochrany osobních údajů na národní úrovni (například působnost a organizaci Úřadu pro ochranu osobních údajů), těžiště právní úpravy však zůstane v GDPR. Ruší také současný zákon o ochraně osobních údajů. Smyslem je tedy zabránit zmatkům, které by mohly vzniknout v případě účinnosti jak stávajícího zákona, tak GDPR. Bohužel Česká republika přípravy podcenila, ať už jde o metodiku nebo přípravu adaptačního zákona. Například v Německu již minulá vláda přijala jejich adaptační zákon a tento nabude účinnosti 25. 5. 2018.

Bude však k dispozici dostatek kapacit kontrolovat dodržování stanovených norem?

PROSAZOVÁNÍ NOVÉHO NAŘÍZENÍ

Schválení legislativy není konec, ale teprve začátek celého procesu. Podmínkou existence jakéhokoliv právního systému je totiž jeho schopnost pravidla vynucovat. Bude však k dispozici dostatek kapacit kontrolovat dodržování stanovených norem? Úřad pro ochranu osobních údajů se domnívá, že ano. Bude se ale zřejmě při kontrolách zaměřovat hlavně na dodržování nejdůležitějších povinností a kontroly provádět na základě podnětů. Jako ale celá veřejná správa, i úřad má problém udržet si zaměstnance, kteří jsou profesionály v dané oblasti, zejména kteří rozumějí informačním technologiím. Po zapracování tito zaměstnanci často odcházejí do soukromého sektoru, kde mají vyšší příjmy.

ZÁKLADNÍ PRINCIPY GDPR

GDPR je založeno na dvou základních principech: na principu odpovědnosti a přístupu založeném na riziku. Princip odpovědnosti znamená odpovědnost správce za dodržení zásad zpracování osobních údajů, které jsou stanoveny GDPR, a schopnosti soulad prokázat. Princip založený na riziku znamená, že správce musí od počátku zpracování brát v potaz rizika pro práva a svobody subjektů údajů, která s tímto zpracováním souvisejí. V užším smyslu je aplikace některých povinností stanovených GDPR podmíněna existencí rizika (například v případě vysokého rizika). Oba principy se uplatní současně.

Jelikož ani GDPR se nevyhnulo různým mýtům a nepravdám, setkali jsme se v rámci naší praxe i s názory, kterými by se firmy rozhodně neměly řídit. Jedním z takových názorů je představa, že si správce může vybrat, zda se bude řídit principem odpovědnosti nebo přístupem založeným na riziku. Pokud si podle tohoto názoru zvolí „princip odpovědnosti“, musí dodržet

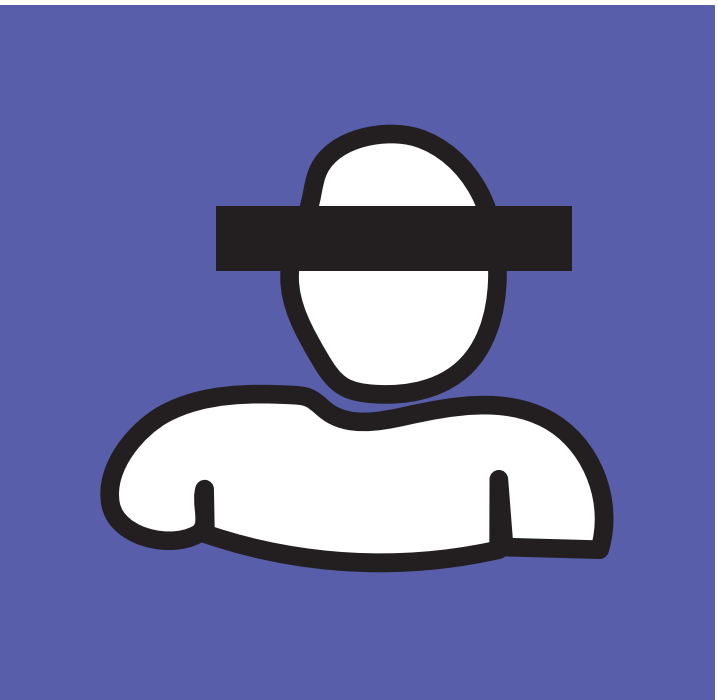
všechny povinnosti stanovené GDPR. Pokud si zvolí „přístup založený na riziku", uplatní se pouze některé povinnosti stanovené GDPR, avšak s vyšším rizikem postihu v případě narušení ochrany osobních údajů. Takový názor samozřejmě nemá oporu v GDPR.

NEJEN POVINNOSTI, ALE I PŘÍLEŽITOSTI

Pro firmy je důležité pochopit rizika a nové povinnosti související se zpracováním osobních údajů, kterým budou čelit. Mezi významné změny patří:

- nová práva subjektů údajů, jako například rozšíření práva být zapomenut, právo na přenositelnost osobních údajů, právo na bezplatnou první kopii osobních údajů,
- náročnější požadavky na zajištění organizačních a technických opatření,
- povinnost zpracovat posouzení dopadu na ochranu osobních údajů,
- povinnost ustavit roli pověřence pro ochranu osobních údajů,
- detailní náležitosti smlouvy o zpracování osobních údajů uzavřené mezi správcem a zpracovatelem,
- širší informační povinnost vůči subjektům údajů,
- přísnější požadavky na podobu souhlasu a výslovně stanovené právo souhlas odvolat.

GDPR nepřináší jen nové povinnosti. V některých případech může být zpracování osobních údajů snazší.



GDPR nepřináší jen nové povinnosti. V některých případech může být zpracování osobních údajů snazší. Jedním z titulů, kterými může podle aktuální právní úpravy firma podložit zpracování osobních údajů, je ochrana práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Zákon o ochraně osobních údajů hned druhým dechem stanoví, že takové zpracování osobních údajů nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.

GDPR přináší podobný titul pro zpracování osobních údajů, a to oprávněné zájmy příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

„Ochranu práv a právem chráněných zájmů" podle zákona o ochraně osobních údajů je třeba vykládat jako zájem správce uznaný právním řádem, tedy nikoliv jako subjektivní názor správce. Naproti tomu GDPR nově umožňuje založit zpracování na základě „oprávněných zájmů", které nemusí být uznány právem jako konkrétní subjektivní práva (či nároky) správce. GDPR tak umožňuje na základě právního titulu „oprávněných zájmů" zpracovávat osobní údaje z více důvodů a zahrnout tak pod tento titul více zpracovatelských operací. Mezi taková zpracování pak může patřit například přímý marketing, prevence podvodů, předávání osobních údajů v rámci skupiny podniků nebo síťová bezpečnost.

KDE ZAČÍT?

Co je tedy třeba udělat, aby firma ošetřila rizika spojená s novou právní úpravou? Níže uvádíme tipy z praxe, které mohou firmu nasměrovat v rámci projektu implementace GDRP.

- Stanovte odpovědnost za ochranu osobních údajů v organizaci
- Promítněte zásady ochrany osobních údajů do každodenní činnosti organizace
- Zvyšujte povědomí v oblasti ochrany osobních údajů
- Vytvořte přehled o zpracování osobních údajů – registr osobních údajů
- Zaveďte bezpečnostní opatření pro zamezení zneužití údajů s ohledem na riziko
- Upravte smlouvy s dodavateli (zpracovateli osobních údajů)
- Komunikujte a připravte se na situace, kdy se něco nepovede
- Prověřte, zda se vaší společnosti týká povinnost zřídit roli pověřence pro ochranu osobních údajů ☒

O autorovi:
Stanislav Klika pracuje pro BDO jako senior manažer a zaměřuje se na ochranu osobních údajů, vnitřní kontroly, řízení rizik, interní audit a profesní rozvoj interních auditorů.