

Jak velký je ten strašák GDPR?

V posledních dnech je o GDPR, neboli obecném nařízení o ochraně osobních údajů, velmi slyšet. Málokdo však skutečně ví, co se za novými pravidly skrývá a jak se na ně připravit.

Z průzkumů vyplývá, že celá řada podnikatelských subjektů není na nová pravidla připravena. Hospodářská komora ČR předpokládá, že až pětina českých firem není zcela připravena na termín 25. května, kdy začnou nová pravidla platit.

Nařízení je celoevropsky přímo závaznou komplexní právní regulací, která výrazně zvýší ochranu osobních dat občanů. Pravidly se musí řídit ti, kteří shromažďují nebo zpracovávají citlivé osobní údaje. Nezáleží tedy na předmětu podnikání, ale na způsobu, objemu a typu dat, se kterými daný subjekt nakládá. Filozofií GDPR je dle vyjádření eurokomisařky Jourové uklidit si svá data v organizaci či ve firmě a dát si na dveře dvojitý bezpečnostní zámek.

Každý podnikatel by si tedy měl provést „inventarizaci“ dat, která má k dispozici a posoudit, zda existuje riziko jejich úniku. Firmy, které s daty obchodují, přeprodávají a sbírají data o konkrétních osobách, musí přijmout patřičná opatření vyplývající z GDPR. Dle Jiřího Žúrka z Úřadu pro ochranu osobních údajů se nejedná o revoluci, ale o přirozenou evoluci pravidel, která jsou v ČR již nyní stanovena zákonem o ochraně osobních údajů, potažmo směrnicí.

Revize současných pravidel byla motivována digitálním vývojem, a proto tento sektor více zasáhne. Nově GDPR začíná řešit online identifikátory a IP adresy. Za výzvu pro tento sektor, ale i jiné, lze určit skutečnost, že nařízení nestanovuje rozsáhlé výjimky pro malé firmy. V digitálním světě se běžně setkáváme s firmami o jednom či dvou zaměstnancích, kteří nakládají s velkým objemem citlivých dat. Proto i malá firma, která s daty obchoduje, bude muset do svého podnikání investovat zpět část vydělaných peněz právě na ochranu dat.

Jedinou výjimkou pro malé firmy je úleva z evidenční povinnosti vést záznamy o činnostech zpracování dat (do 250 zaměstnanců), a to pro firmy, které s údaji nepracují systematicky a ne rizikovým způsobem. Dle Terezy Šamanové ze Svazu průmyslu a dopravy ČR bude tato výjimka uplatňována pouze ve výjimečných případech. Upozorňuje však na nešvar, který se rozmohl v ČR a desinformaci, že musí mít pověřenci pro ochranu osobních údajů certifikaci. V nařízení není stanovena, a ani v národní legislativě nebude, povinná certifikace pověřenců.

Další výzvou je nejasný výklad některých ustanovení. Komise v lednu přišla s praktickou pomůckou k GDPR a své pokyny také pravidelně vydává pracovní skupina při Evropské komisi WP29 složená z národních expertů. Tyto pokyny je ale potřeba zpřesnit na národní úrovni. Naše vláda dosud nepřipravila český implementační zákon, který by evropské nařízení upřesnil pro české podmínky a pomohl subjektům, kterých se GDPR týká, vyjasnit, co a jak musí splňovat. Laxní přístup je celoevropský fenomén. Do poloviny března přijaly národní právní změny pouze 2 členské státy. Komisařka Jourová slíbila, že bude kritická ke státním orgánům, které neprovedly patřičné právní úpravy. Nařízení platí sice plošně, ale je zde dle jejího názoru prostor pro flexibilitu. Členské státy by například mohly přijít se speciální úpravou pro úřady, na které se stejně jako na jiné subjekty nařízení vztahuje.

Mgr. Ing. Alena Mastantuono, ředitelka CEBRE – České podnikatelské reprezentace při EU