

11. 10. 2017

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

## Zavedení GDPR ve firmě. Jak na to? - 1. část

Již od 25. 5. 2018 vstoupí v platnost Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů. Jedná se o extrémní změnu pro všechny organizace přinášející zásadní posílení ochrany osobních údajů a řadu nových povinností nebo změny stávajících povinností pro všechny správce a zpracovatele osobních údajů. Jaké kroky učinit ve vaší firmě, tak aby vás nepřekvapil zásah úředníků vymáhajících dodržování nové evropské směrnice?



**DITTRICH & CO.**  
advokátní kancelář

*„Obecné nařízení o ochraně osobních údajů, GDPR, bylo přijato 27. 4. 2016 a začne platit za necelý rok. Bude zapotřebí realizovat nákladné a náročné změny ve vašich informačních systémech a interních procesech organizací. Není na místě být překvapení - povinnost zpracování údajů máte i dle české legislativy, a to dle stávajícího zákona č. [101/2000 Sb.](#), o ochraně osobních údajů v platném znění,“* vysvětluje legislativní rámec nařízení EU **Mgr. Michal Dittrich, advokát se specializací na obchodní a podnikové právo.**

### **Konkrétní dopady gdpr směrnice na firmy**

Řečeno stručnou formou, GDPR rozšiřuje nutnost aktivního souhlasu subjektů o nakládání s jejich osobními údaji. Důraz je kladen především na zvýšení zabezpečení dat, např. prostřednictvím datového šifrování. Dále směrnice zavádí nová práva na přístup, přenositelnost a na výmaz údajů. To přináší do struktury organizací technicky náročné změny.

*„Firmy budou nuceny realizovat změny v organizační struktuře, např. zřídit pozice tzv. „pověřence pro ochranu osobních údajů“ neboli „data protection officer“, zkráceně DPO. Součástí je i povinnost řídit se principy tzv. „privacy by design“, což představuje povinné posuzování dopadů významnějších projektů či organizačních rozhodnutí na ochranu osobních údajů,“* říká **Mgr. Michal Dittrich.**

Firmám GDPR přináší povinnost změn dodavatelských smluv a kontraktů z hlediska zpracování osobních údajů, budou muset také proškolit zaměstnance o nových povinnostech a pravidlech. GDPR se též dotkne platebních služeb (nařízení o e-privacy).

### **Jak implementovat gdpr ve vaší organizaci?**

Nejlépe zvolený postup pro případ, že vaší organizaci navštíví komisař, který provede šetření dodržování evropského nařízení GDPR, je připravit se na všechny eventuality dopředu. Byť se jedná o citelný krok pro každou organizaci, může vás ochránit před existenčními problémy v podobě nemalých pokut v řádech tisíců eur.

Zavedení GDPR započnete analýzou stávajícího stavu ověření principů zpracování a bezpečné ochrany dat prostřednictvím bezpečnostního auditu. Pokud jste organizace, kde funguje oddělení bezpečnosti (security department), můžete interní audit realizovat svými silami. V opačném případě si najměte externí auditory. Provedení auditu je dnes v nabídce advokátních kanceláří i konzultačních společností.

Cílem auditu by mělo být získání přehledu o tom, jaká zpracování údajů provádíte, hlavně v oblasti zpracování a uchování osobních údajů a dat vašich klientů. Odpovězte si na dotaz, jestli je tato agenda vedena manuálně anebo automatizovaně. Ověřte, na základě jakého právního titulu a v jakém rozsahu osobní údaje zpracováváte. Nejčastěji to bude k úkonům plnění smluv, plnění podnikatelského záměru atd.

*„Audit by měl určit i přesnou periodicitu likvidace osobních údajů. Uchováváte data pouze po dobu nezbytně nutnou nebo dlouhodoběji? Jak dochází k obnově aktuálnosti údajů? Popište tedy přesně interní procesy zpracování a uchování dat. Pokud k nim nedochází, opatření a procesy zaveďte,“* radí **Mgr. Michal Dittrich**. Úředníky bude zajímat i určení povinnosti, kdo je za dodržení normy ve vaší organizaci odpovědný a kdo se subjekty daných údajů na přímo komunikuje. Samozřejmostí je i zjištění, zda-li jsou data někomu dalšímu přístupná, a to jak v rámci vaší firmy, tak i v případě vašich obchodních partnerů.

Součástí řízení s vaší společností bude i prověření, jestli chráníte dostatečně osobní údaje. Máte bezpečnostní oddělení a nastavené procesy ochrany dat. Zjišťování stavu bezpečnosti v organizaci se bude týkat i nastavení bezpečnosti techniky (PC, telefony, tablety, komunikátory) vedoucí k prověření, jestli nemůže nastat situace nahodilého přístupu k osobním údajům, jejich změně, zničení nebo ztrátě.

Třešničkou na dortu může být požadavek na předložení interní dokumentace, která celou agendu zpracování dat zastřešuje.

### **Co se stane, když gdpr ve firmě nezavedeme?**

Podle Mgr. Michal Dittricha je nepodřízení se všeobecnému nařízení GDPR spojeno s výraznými sankcemi. *„Pokuty se mohou pohybovat v milionech EUR. Přitom je nutné počítat s tím, že evropské úřady budou maximalizovat tlak na jednotné vymáhání práva ve všech státech, což se odrazí v unifikování výše pokut pro celou Evropskou unii,“* říká **advokát Mgr. Michal Dittrich**.

V příštím díle článku se zaměříme na zavedení interního systému reportingu dodržování GDPR v organizaci.

**Mgr. Michal Dittrich**

[DITTRICH & CO. - advokátní kancelář s.r.o.](#)

Na Březince 930/6  
150 00 Praha 5 - Smíchov

Tel.: +420 222 560 060

e-mail: [office@akdf.cz](mailto:office@akdf.cz)

© EPRAVO.CZ - Sběrka zákonů, judikatura, právo | [www.epravo.cz](http://www.epravo.cz)

## Další články:

- [Nový zákon o veřejných dražbách, aukce a obálkové metody](#)
- [Pohled přes hranice - natáčení pornografických klipů jako důvod výpovědi z nájmu bytu](#)
- [Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi](#)
- [Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi](#)
- [Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny](#)
- [Druhá „tlačítková novela“: povinné tlačítko pro odstoupení od smlouvy](#)
- [Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení - nález Ústavního soudu sp. zn. I. ÚS 2541/25](#)
- [Kupní smlouva bez přesného určení kupní ceny](#)
- [Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti](#)
- [Detekce podezřelého obchodu v kontextu hazardních her](#)
- [AI omnibus](#)