

Od mája 2018 musia všetky slovenské spoločnosti plniť nové všeobecné nariadenie EÚ o ochrane osobných údajov (GDPR).

Za nedodržanie pravidiel hrozia sankcie až do výšky 4 % výnosov.

Ste pripravení  
na zmenu?

[kpmg.sk](http://kpmg.sk)



# **KPMG** *Všeobecné nariadenie o ochrane údajov (GDPR)* *Prehľad*

Nariadenie EÚ reaguje na obavy, ktoré ako jednotlivci máme v súvislosti s tým, ako spoločnosti používajú naše osobné údaje. Prispôsobenie sa prísnejším pravidlám však pre tieto firmy predstavuje významnú výzvu.

Môžu mať totiž vplyv na takmer každú činnosť vašej spoločnosti od HR cez oddelenie predaja až po oddelenie financií, ako aj na váš dodávateľský reťazec a základné IT systémy. Firmy zároveň nesú novú zodpovednosť a ak nedodržia svoje povinnosti, hrozia im nezanedbateľné pokuty a sankcie.

Spolu s mojím tímom v KPMG pomáhame firmám efektívne a účinne sa prispôbiť regulačným požiadavkám. Rád sa s vami stretnem a osobne môžeme prediskutovať vaše otázky spojené s ochranou osobných údajov, preskúmam výzvy, ktorým čelíte, a spoločne pripravíme praktické a včasné riešenia.

Pokojne ma kontaktujte priamo a pomôžem vám zhodnotiť, či a ako sa na vás nariadenie vzťahuje. Prípadne sa obráťte na svojho kontaktného manažéra z KPMG, ktorý vás s nami spojí.

Tešíme sa na vašu odpoveď.



**Pavol Adamec**

Vedúci oddelenia pre riadenie rizík  
KPMG na Slovensku

20 rokov skúseností s prácou  
so slovenskými právnymi predpismi

**T:** +421 904 702 339

**E:** padamec@kpmg.sk

**kpmg.sk**



# Často kladené otázky

## Čo prináša toto nové nariadenie?

Toto nariadenie kladie právnu zodpovednosť na spoločnosti za spravovanie osobných údajov o súkromných osobách, ktoré uchovávajú a spracovávajú, podľa nového definovaného rámca.

## Čo je nové oproti súčasnému stavu?

Súčasný stav, založený na smerniciach EÚ z roku 1995, kládol dôkazné bremeno na jednotlivca alebo regulačný orgán, aby preukázali, ako spoločnosť zneužila ich osobné údaje. Nové nariadenie, plne účinné od roku 2018, jednoznačne kladie zodpovednosť na spoločnosť za to, aby preukázala, že nezneužila uchovávané osobné údaje. Ide o zásadný posun v celkovom vnímaní a každá spoločnosť musí túto zmenu implementovať.

## Ktorých osôb sa to týka?

Definícia je široká a vzťahuje sa na akúkoľvek osobu. Môže zahŕňať tých, ktorí majú nejaký vzťah s vašou spoločnosťou, čiže vašich zamestnancov, zákazníkov alebo dodávateľov, ale aj kandidátov, ktorí vám pošlú životopis. Zahŕňa však aj tie osoby, ktoré s vami nemajú žiadny vzťah, ako napríklad pri prieskume trhu.

## Čo sa považuje za osobné údaje?

Všetky údaje, ktoré môžu identifikovať jednotlivca. Platí to napríklad pre meno, adresu, telefónne číslo či e-mail.

## Ako by to v praxi mohlo ovplyvniť moju spoločnosť?

Každá osoba sa môže obrátiť na vašu spoločnosť a opýtať sa, ktoré osobné údaje o nej spracovávate a/alebo požadovať formálne vyjadrenie, že o nej neuchováate žiadne osobné údaje. Ak spracovávate takéto informácie, musíte potvrdiť, čo uchováate, ako ich používate, a ak o to jednotlivec požiada, vymazať ich.

## Vzťahuje sa toto nariadenie na moju spoločnosť?

Ak spracovávate údaje o svojich zamestnancoch, podrobnosti o zákazníkoch a/alebo o ich vernostných programoch alebo údaje o pracovníkoch dodávateľov, pravdepodobne sa toto nariadenie týka práve vás.

## Ako aktuálne pristupujú slovenské spoločnosti k tejto téme?

Veľké spoločnosti typu B2C, ako napríklad finančné služby, maloobchodníci a telekomunikácie, pracujú na zefektívnení podnikových procesov (tzv. reengineering) už zhruba 18 mesiacov. Spoločnosti typu B2B v súčasnosti pripravujú analýzy dôsledkov novej legislatívy, čím začali alebo začínajú proces reengineeringu. Dátum účinnosti je 25. máj 2018.



## **Vzťahuje sa nariadenie len na veľké spoločnosti?**

Nariadenie sa vzťahuje na všetky typy slovenských spoločností. S osobitným dôrazom sa zameriava na tie, ktoré spracovávajú veľké množstvo osobných údajov. V súčasnosti však nariadenie neupresňuje, ako a či vôbec bude rozlišovať podľa veľkosti. Aktuálne sú všetky spoločnosti vnímané rovnocenne.

## **Kto a ako často bude kontrolovať dodržiavanie nariadenia?**

Zodpovednosť za zabezpečenie dodržiavania nariadenia spadá do kompetencie Úradu na ochranu osobných údajov SR, nezávislému orgánu, ktorý sa zodpovedá priamo parlamentu SR.

## **Čo sa stane, ak požiadavky nespĺníme?**

Nedodržanie požiadaviek môže viesť k pokutám až do výšky 20 miliónov € alebo 4 % celosvetového ročného obratu. Sankcie ukladá Úrad na ochranu osobných údajov SR.

## **Na dosiahnutie súladu s nariadením musí mať spoločnosť postupy, aby dokázala vykonať nasledovné činnosti:**

1. Identifikovať všetky osobné údaje uchovávané o jednotlivcovi v celej spoločnosti.
2. Poskytnúť jednotlivcom na základe ich žiadosti všetky osobné údaje, ktoré o nich spoločnosť spracováva.
3. Identifikovať prípady porušenia ochrany údajov, napríklad únik údajov, stratu údajov a neschopnosť splniť požiadavku jednotlivca.
4. Zozbierať, posúdiť a ohlásiť prípady porušenia ochrany osobných údajov Úradu na ochranu osobných údajov SR do troch dní odo dňa, keď sa o nich dozvie.
5. Zabezpečiť súhlas od všetkých osôb, ktorých osobné údaje uchováva a spracováva.
6. Spravovať individuálne žiadosti o poskytnutie alebo vymazanie uchovávaných údajov.
7. Mať vymenovanú osobu zodpovednú za dohľad nad spracovávaním osobných údajov v spoločnosti.
8. Preukázať, že má efektívny systém riadenia bezpečnosti osobných údajov.

## **Ako zabezpečím prispôsobenie svojej spoločnosti nariadeniu?**

Prvým krokom je vypracovanie analýzy všetkých dôsledkov s cieľom posúdiť, či sa nariadenie vzťahuje na vás a ak áno, v akých oblastiach a či sú vaše súčasné opatrenia adekvátne. Je potrebné implementovať identifikované zmeny ako aj zabezpečiť priebežnú aktualizáciu vašej dokumentácie a opatrení s cieľom byť schopný preukázať, že zmeny vášho prostredia a interných postupov negatívne neovplyvňujú vašu schopnosť dodržiavať nariadenia. Na vyžiadanie by mala byť vaša interná dokumentácia prístupná na kontrolu Úradu na ochranu osobných údajov SR. Tento proces môžete realizovať interne alebo pomocou externého poskytovateľa služieb.

## **Kto by mal byť v mojej spoločnosti za túto oblasť zodpovedný?**

V konečnom dôsledku je zabezpečenie súladu zodpovednosťou štatutárov a vrcholového manažmentu. Dodržiavanie nariadenia ovplyvňuje mnoho rôznych aspektov organizácie, a teda sa týka viacerých členov vrcholového manažmentu zastupujúcich jednotlivé oddelenia spoločnosti. Tí musia byť dostatočne informovaní a poučení, aby sa docielilo dodržiavanie nariadenia naprieč celou spoločnosťou.



# Ako vám KPMG môže pomôcť – osvedčená metodológia

| Štádium                                                                              | Cieľ                                                                                                                                                                                                                                                             | Váš výstup                                                                                                                                         |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sken<br/>Workshop</b>                                                             | Na moderovanom workshope s predstaviteľmi tých funkcií, ktoré nariadenie pravdepodobne zasiahne (HR, predaj, obstarávanie, IT a financie) poukážeme na kľúčové požiadavky a spolu s vaším tímom identifikujeme kľúčové procesy, ktorých sa nové pravidlá dotknú. | Posúdenie aplikovateľnosti nariadenia a identifikácia kľúčových procesov, ktoré ovplyvní.                                                          |
| <b>Analýza</b>                                                                       | Podrobne porovnáme aktuálny stav vašich procesov s novými pravidlami a zmapujeme spôsoby spracovania osobných údajov. Zohľadníme pri tom interné procesy, systémy spracovávajúce osobné údaje, interné štandardy a postupy, ako aj ďalšie relevantné dokumenty.  | Posúdenie nedostatkov, ktoré odhalia špecifické rozdiely medzi aktuálnymi a požadovanými procesmi.                                                 |
| <b>Návrh<br/>budúceho<br/>stavu</b>                                                  | Navrhujeme príslušné opatrenia potrebné na zosúladenie s novými pravidlami vrátane zmien procesov. Definujeme požiadavky na IT systémy. Stanovíme priority, vyhodnotíme náročnosť a navrhujeme plán realizácie.                                                  | Plán realizácie, kde budú špecifikované zmeny procesov a IT systémov, rozdelená zodpovednosť za jednotlivé úlohy a stanovený časový plán projektu. |
| <b>Podpora<br/>pri imple-<br/>mentácii</b>                                           | Podporíme vašich interných manažérov pri realizácii zmien v existujúcich systémoch alebo pri integrácii nových systémov do vašej existujúcej architektúry.                                                                                                       | Monitorovanie, podpora a plnenie pridelených úloh pri implementácii plánu.                                                                         |
| <b>Priebežná<br/>údržba a<br/>testovanie<br/>dodržiava-<br/>nia naria-<br/>denia</b> | Posúdiť vplyv systémových zmien na dodržiavanie nariadenia. Posúdiť vplyv akýchkoľvek regulačných zmien alebo objasnení postupov.                                                                                                                                | Odhad nedostatkov a návrh možností na ich nápravu. Správa o dodržiavaní predpisov, ktorú možno poskytnúť dozornému orgánu.                         |
| <b>Zodpovedná<br/>osoba<br/>(Data<br/>Privacy<br/>Officer)</b>                       | Zabezpečiť dodržiavanie právnych predpisov v rozsahu úloh a povinností zodpovednej osoby.                                                                                                                                                                        | Kvalifikovaná personálna kapacita schopná vykonávať požadované úkony krátkodobo alebo dlhodobo.                                                    |



# Dôverujte KPMG pri prispôsobovaní sa novým právnym predpisom

## **Pavol Adamec**

Vedúci oddelenia pre riadenie rizík  
KPMG na Slovensku

**T:** +421 904 702 339

**E:** padamec@kpmg.sk

## **KPMG Slovensko spol. s r.o.**

Dvořákovo nábrežie 10  
811 02 Bratislava

Žriedlová 12-14  
040 01 Košice

**T:** +421 2 5998 4111

**F:** +421 2 5998 4222

**E:** kpmg@kpmg.sk

**kpmg.sk**



© 2018 KPMG Slovensko spol. s r.o., slovenská spoločnosť  
s ručením obmedzeným a člen KPMG, siete nezávislých  
firiem pridružených ku KPMG International Cooperative,  
právnickej osobe registrovanej vo Švajčiarsku.  
Všetky práva vyhradené. Vytlačené na Slovensku.