25. 4. 2018

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

GDPR: jak efektivně implementovat za „pět minut dvanáct“?

Dne 25. 5. 2018 nabývá účinnosti nové evropské obecné nařízení o ochraně osobních údajů známé pod anglickou zkratkou GDPR. Podnikatelům, společnostem a ostatním správcům osobních údajů tak zbývá již pouze několik týdnů na přípravu a zajištění souladu.

dvořák || hager & partners
advokátní kancelář

I když značná část firem v tomto procesu už výrazně pokročila nebo je dokonce před jeho dokončením, stále existuje nezanedbatelné množství organizací, které jsou teprve na startu nebo těsně za ním.

Připravili jsme proto shrnutí našich zkušeností a doporučení z mnoha realizovaných GDPR projektů tak, aby většina běžných obchodních či výrobních firem, u kterých zpracování osobních údajů hraje pouze podpůrnou roli, byla schopna dosáhnout ve zbývajícím čase alespoň uspokojivé úrovně souladu s GDPR.

Mapování je základ

Prvním krokem přípravy na GDPR je **identifikace a zmapování veškerých procesů zpracování osobních údajů**, které ve firmě provádíte. Nemusí se jednat o žádné sofistikované postupy, ale v podstatě stačí zodpovězení základních „kriminalistických“ otázek pro každé zpracování identifikované dle jeho účelu:

- kdo (jsme správce nebo zpracovatel),
- co (jaké údaje zpracováváme),
- proč (za jakým účelem a na základě jakého zákonného důvodu),
- o kom (koho se údaje týkají), komu (komu mohou být údaje zpřístupněny),
- kdy (jak dlouho údaje držíme) a
- jak (jak údaje zpracováváme a chráníme).

V optimálním případě by výstupem této mapovací fáze měl být přehled zpracování osobních údajů, který bude možné následně využít jako podklad pro záznamy o zpracování osobních údajů podle GDPR.

Provedení rozdílové analýzy

Pokud máte zmapovány procesy zpracování ve společnosti, přichází další krok spočívající v porovnání současného stavu se šesti povinnostmi každého správce osobních údajů dle GDPR.

Především je tak nutné prověřit, zda používáte pro dané zpracování správný zákonný důvod

(zákonnost). Zvláštní pozornost je potřeba věnovat souhlasu s ohledem na zpřísnění požadavků pro jeho získání a udržení**. Souhlas jako zákonný důvod zpracování doporučujeme využívat pouze tehdy, pokud skutečně nemůžete využít jiný zákonný důvod (plnění právní povinnosti, uzavření či plnění smlouvy nebo oprávněný zájem správce).**

Po stanovení správného zákonného důvodu následuje prověření, zda veškeré údaje, které zpracováváte, jsou nezbytné pro legitimní a předem stanovený účel zpracování (omezení účelem), a zda je uchováváte pouze po nezbytnou dobu (minimalizace údajů a doby uchování). Je také nutné zabezpečit, abyste zpracovávali pouze přesné a podle potřeby aktualizované osobní údaje (přesnost).

Dále je potřeba podívat se na informace, které subjektům údajů o zpracování poskytujete a jakým způsobem budete reagovat na jejich související žádosti a práva a napomáhat jim při jejich výkonu (transparentnost a férovost). Ve většině případů stávající informace nebudou odpovídat požadavkům GDPR na obsah i formu. Obvykle ve firmách absentují také procesy, jak budou reagovat na žádosti subjektů.

Konečně je nutné zhodnotit rizikovost každého zpracování a přijmout a zdokumentovat odpovídající technická a organizační opatření k ochraně zpracování před neoprávněným přístupem či zpracováním a před náhodnou ztrátou, zničením nebo poškozením údajů (integrita a důvěrnost).

A konečně samotná implementace

Doporučujeme, abyste na základě zjištěných nedostatků stanovili konkrétní nápravná opatření zajišťující soulad s GDPR. S ohledem na čas je nutné identifikovat priority pro implementaci a přijmout odpovídající harmonogram.

V každém případě je možné předpokládat, že se nevyhnete následujícím v podstatě „standardním“ implementačním opatřením:

- vytvoření nebo aktualizace evidence zpracování (záznamů o zpracování),
- přijetí nové nebo revidované interní dokumentace, a to zejména v oblasti HR (vstupní dotazníky, pracovní smlouvy, směrnice pro nakládání s osobními údaji, informace pro zaměstnance),
- přijetí nové nebo revidované externí dokumentace (oznámení o zpracování, souhlasy s přímým marketingem, obchodní podmínky),
- revize a doplnění smluv se zpracovateli (typicky externí mzdová účtárna nebo bezpečnostní agentura či poskytovatelé benefitů),
- provedení základní rizikové analýzy (vč. zhodnocení případné potřeby jmenování pověřence nebo detailnějšího posuzování vlivu zpracování),
- dokumentace technických a organizačních opatření k zabezpečení zpracování vč. nastavení interních procesů (reakce na žádosti a výkon práv, ohlašování a dokumentace incidentů atd.),
- školení a testování zaměstnanců.

Tento výčet není vyčerpávající a představuje pouze standardní základní „implementační balíček“. Konkrétní rozsah implementačních opatření se bude vždy lišit zejména podle rozsahu, povahy, kontextu a účelu zpracování. V každém případě se jedná o obvyklé minimum, které z velké části můžete řešit ve zbývajícím čase.

I pokud se případně nepodaří vše stihnout do účinnosti GDPR, není nutné, abyste propadali beznaději a pasivně čekali na masivní pokutu! Je zcela legitimní očekávat, že zmapování zpracování, částečná implementace priorit a reálný harmonogram pro zbývající opatření budou vždy

zohledněny v případě kontroly a měly by vás uchránit před uložením nějaké zásadní sankce.

Radek Matouš
vedoucí advokát

Dvořák Hager & Partners, advokátní kancelář, s.r.o.

Oasis Florenc
Pobřežní 394/12
186 00 Praha 8

Tel.: +420 255 706 500
e-mail: praha@dhplegal.com

Další články:

- Přezkum rozhodnutí CAS vnitrostátními soudy Evropské unie
- Právo na soukromí vs. transparentnost firem: Kontroverze kolem evidence skutečných majitelů
- GDPR 2.0: Jednodušší regulace pro odvážnou a konkurenceschopnou Evropu?
- Důkladnější přezkum rozhodnutí vydaných Rozhodčím soudem pro Sport
- Novinky z české a evropské regulace finančních institucí za měsíc červen 2025
- Digitální marketing: Rozhodnutí belgického soudu ve věci IAB Europe
- Evropská zdravotní data pod lupou: Co přináší nová regulace a datová centra (EHDS)?
- Novinky z české a evropské regulace finančních institucí za měsíc květen 2025
- Úvodní vhled do klasifikace povinných osob dle návrhu nového zákona o kybernetické bezpečnosti
- Nový zákon o kybernetické bezpečnosti: co se mění a jak se připravit?
- Ohrožení pobídek v modelu bez investičního poradenství?