Doporučení kroků, které podniknout za účelem vyhovění požadavkům GDPR

Tento dokument navazuje na prezentaci vytvořenou HÁJEK ZRZAVECKÝ advokátní kancelář, s.r.o. ve spolupráci s Českomoravským svazem minipivovarů a má za cíl poskytnout členům svazu stručný přehled kroků a opatření, které je obecně vhodné uskutečnit a provést k tomu, aby jejich minipivovar, resp. společnost či fyzická osoba, která jej provozuje, mohl vyhovět požadavkům **nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)** (dále jen **„GDPR"**).

Každý minipivovar, resp. společnost či fyzická osoba, která jej provozuje, bude podle GDPR v určitých případech zpracování osobních údajů fyzických osob považován za správce a/nebo i zpracovatele osobních údajů a musí tak plnit povinnosti, které mu z GDPR vyplývají.

Pro jednotlivé oblasti témat, jak jsou předestřeny ve výše zmíněné prezentaci, si v tomto dokumentu dovolujeme nabídnout přehled doporučených kroků a vybraných opatření, které mohou směřovat k zajištění souladu s GDPR.

ZÁKLADNÍ POJMY A DEFINICE

Každý minipivovar by měl v první řadě **provést základní audit aktuálního stavu zpracování osobních údajů**:

1. Zjistit, jaké osobní údaje při svých činnostech zpracovává (identifikovat jejich kategorie).
2. Zjistit, pro jaké účely takové osobní údaje zpracovává (identifikovat jednotlivé účely).
3. Zjistit, jaké subjekty údajů jsou dotčeny takovými procesy zpracování (identifikovat jejich kategorie).
4. Provést katalogizaci či vytvořit přehled/třídění takových procesů zpracování, účelů, osobních údajů zpracovávaných a subjektů údajů zpracováním dotčených.
5. Identifikovat veškeré ostatní správce a zpracovatele, se kterými udržuje nějaké právní vztahy a popsat jejich účel a princip.
6. Identifikovat veškeré další osoby mimo minipivovar, které by mohly či mají k osobním údajům přístup.

ZÁSADY A ZÁKONNOST ZPRACOVÁNÍ

Minipivovar by měl dále **posoudit dodržování základních zásad a zákonnosti zpracování osobních údajů**:

1. Pro jednotlivé identifikované účely a procesy zpracování definovat přiléhající právní tituly (důvody) zpracování.
2. Posoudit rozsah jednotlivých procesů zpracování a nutnost zpracování konkrétních osobních údajů a dobu jejich uchování.
3. Stanovit doby uchování osobních údajů.
4. V případě, že provádí zpracování na základě právního titulu – oprávněného zájmu provést balanční test možnosti zpracování.

5. V případě, že provádí zpracování na základě právního titulu – souhlasu:
    a. posoudit, zda je užití souhlasu opravdu vhodné a nutné.
    b. zrevidovat stávající souhlasy a vytvořit souhlasy nové.
    c. je-li to třeba, vyžádat si souhlasy nové.
    d. umožnit jednoduché odvolání udělených souhlasů.
6. Posoudit rizika jednotlivých procesů zpracování a nastavit postupy jejich posouzení pro nové procesy.

PRÁVA SUBJEKTŮ ÚDAJŮ

Dále by měl minipivovar **provést úpravy a zavést nové přístupy v oblasti práv subjektů údajů**:

1. Zrevidovat a identifikovat stávající postupy pro uplatnění a výkon práv subjektů údajů.
2. Zavést a nastavit nové postupy pro uplatnění a výkon práv subjektů údajů v souladu s GDPR.
3. Připravit prostředky pro uplatnění a výkon práv subjektů údajů (kontaktní formulář, zvláštní e-mailová adresa, webový formulář, vzorové dokumenty).
4. Ve vztahu k právu na informace o zpracování osobních údajů je pak třeba:
    a. zrevidovat stávající informační dokumenty.
    b. zavést a nastavit nové informační postupy a dokumentaci v souladu s GDPR (informační dokumenty pro zaměstnance, zákazníky, Privacy Policy, Cookie Policy apod.).
5. Identifikovat odpovědnou osobu za řešení problematiky a zajistit jeho proškolení.

POVINNOSTI SPRÁVCŮ A ZPRACOVATELŮ

Zbývající, avšak neméně důležitou oblastí, je **posouzení dodržování povinností správců a zpracovatelů**, kde by měl minipivovar:

1. Zavést vhodná technická a organizačních opatření k zajištění souladu s GDPR a rovněž k prokázání souladu s GDPR, které je vyžadováno v případě kontroly, jako jsou zejména:
    a. přehled přijatých opatření,
    b. interní směrnice o ochraně osobní údajů,
    c. revize pracovněprávní dokumentace,
    d. revize všeobecných obchodních podmínek či jiných řádů,
    e. popis interních procesů (informování subjektů, získání souhlasů, naplňování práv subjektů údajů, likvidace a výmazu apod.),
    f. vzorová dokumentace
        i. informační dokument pro zaměstnance,
        ii. informační dokument pro zákazníky,
        iii. souhlasy se zpracováním osobních údajů např. pro marketingová sdělení,
        iv. formuláře pro uplatnění práv subjektů údajů,
    g. veřejná Privacy Policy a Cookie Policy na webu,
    h. školení zaměstnanců,
    i. nastavení a úprava webu,
    j. záznamy o činnostech zpracování,
        i. vytvoření vzorového záznamu,
        ii. vyplnění záznamů pro jednotlivé procesy zpracování,
        iii. určit osobu odpovědnou za vedení záznamů,
    k. pověření zaměstnanců, kteří nakládají s osobními údaji,

l. úprava či vytvoření smluv s ostatními správci a zpracovateli v souladu s GDPR a nastavení pravidel jejich výběru,
m. posouzení nastavení kamerových systémů a vytvoření dokumentace s těmito související, a
n. nastavit proces jejich pravidelné aktualizace a revize.

2. Případně i identifikovat zpracování, která budou vyžadovat provedení DPIA, a v případě jejich výskytu DPIA pro tato zpracování provést.
3. Provést audit zabezpečení dat a zavést dostatečné prostředky zabezpečení (fyzická ochrana, IT ochrana atd.).
4. Nastavit postupy a procesy pro posuzování, ohlašování a oznamování případů narušení zabezpečení osobních údajů.
5. Určit osoby odpovědné za ochranu osobních údajů.
6. Případně provést analýzu, zda není třeba jmenovat DPO.
7. Identifikovat předávání do třetích zemí mimo EU a tyto posoudit, zda jsou v souladu s GDPR, případně identifikovat či zavést vhodné záruky.
8. Identifikovat vhodné poradce, kteří mohou minipivovaru asistovat v případě řešení otázek ochrany osobních údajů se subjekty údajů a/nebo s dozorovým úřadem v rámci kontroly.

Tento dokument slouží jako obecné doporučení vhodného postupu při zajištění souladu malého nebo středního podniku s požadavky GDPR. Nejedná se o vyčerpávající a plně detailní popis postupu pro konkrétní společnost, kdy k vytvoření takového postupu je třeba plně se seznámit s fungování a procesy dané společnosti.

Rádi Vás provedeme jednotlivými kroky za účelem vyhovění požadavkům GDPR, neváhejte se na nás obrátit.

HÁJEK ZRZAVECKÝ advokátní kancelář, s.r.o.

Mgr. Martin Hájek - hajek@hajekzrzavecky.cz
Mgr. Jakub Málek - malek@hajekzrzavecky.cz

Závěry a názory obsažené v tomto dokumentu jsou vyjádřením právního názoru HÁJEK ZRZAVECKÝ advokátní kancelář, s.r.o. Nelze jednoznačně vyloučit, že by se příslušný soud či jiný orgán, který by se danou záležitostí zabýval, mohl přiklonit k názoru odlišnému. Závěry a právní názory obsažené v této analýze reflektují stav dostupných názorů na interpretaci GDPR ke dni jejího odevzdání, avšak je třeba respektovat skutečnost, že GDPR je nový, přímo aplikovatelný předpis EU a neexistuje k němu v současné době žádná judikatura a ani implementační legislativa. Plně aplikovatelné nejsou ani interpretace vztahující se ke stávající právní úpravě. Závěry a právní názory uvedené v této analýze se s ohledem na výše uvedené mohou v čase měnit, a to zejména v návaznosti na českou implementační a sektorovou legislativu, výkladová stanoviska Working Party 29, Evropského sboru pro ochranu osobních údajů, jednotlivých evropských dozorových úřadů a také v návaznosti na rozhodovací praxi českých a evropských soudů.