

Stručný a jasný GDPR manuál pro podnikatele a malé firmy

GDPR přináší dvě novinky. Musíte vědět, **kde ve firmě máte osobní údaje a jak je máte chráněné**. GDPR je obdoba BOZP, jenom je o ochraně osobních údajů.

Tento manuál je určen drobným podnikatelům, kteří shromažďují osobní údaje a používají je výhradně pro svoje podnikání, tj. nikomu je dál neprodávají ani neposílají nevyžádanou poštu. Ostatní by měli radši oslovit specialisty.

Zde je krátce a jasně, co máte udělat, abyste byli v klidu:

1. Začněte tím, že vyplníte formulář na druhé straně.
2. Přijměte opatření, abyste na všechny dotazy odpověděli ANO.
3. Až budete mít hotovo, seznamte zaměstnance s formulářem stejně, jako je seznamujete s novinkami v BOZP.
4. Zákazníci by měli vědět, co a jak děláte s jejich osobními údaji, proto vyplněný formulář klidně pověste na web pod záložku „Chráníme osobní údaje“ nebo i umístěte viditelně v provozovně.
5. Pak už si jenom hlídejte, abyste se nedostali mimo odpovědi ANO.

Dále najdete odpovědi na pár nejčastějších dotazů:

- (a) **Proč je to tak jednoduché?** Protože GDPR vzniklo, aby hlídalo korporace, které ve velkém obchodují s osobními údaji. Základní stanovená pravidla pro malé podniky a živnostníky jsou nastavena tak, aby byla zvládnutelná „selským rozumem“.
- (b) **Co je osobní údaj?** Cokoliv, co jde spojit s konkrétní osobou, např. fotografie, telefonní číslo, e-mail apod. Citlivý osobní údaj je osobní údaj, který může svým nesprávným užitím nositele osobních údajů poškodit, např. zdravotní záznamy.
- (c) **Máme vyhodit vizitky, objednávky, faktury, obchodní korespondenci, kde jsou osobní údaje?** Ani omylem, toto jsou oprávněně shromážděné osobní údaje, buď na žádost (vizitky), dle smlouvy (objednávky), dle zákona (účetnictví/daně) nebo pro účely ochrany oprávněného zájmu v soudním/správním/jiném řízení, či nakonec pro potřeby archivace dle zákona.
- (d) **Jak dlouho mám evidovat osobní údaje?** Po dobu, co trvá poslední z účelů dle (c), takže obvykle 10 let, např. z důvodu ochrany před možným soudním řízením se zákazníkem nebo pro účely archivace dle zákona.
- (e) **Co mám říct zákazníkovi, když chce smazat svoje údaje?** Potvrdit, že je určitě smažete, jakmile Vám uplyne doba evidence dle písm. (d).
- (f) **Jak je to s hlášením úniku ÚOOU (Úřad pro ochranu osobních údajů)?** V klidu. Hlásíte ÚOOU (www.uoou.cz, rubrika Poradna/Jak postupovat) do 72 hodin od úniku pouze závažnější porušení zabezpečení osobních údajů, které mohou poškodit dotčené osoby, jinak pouze podniknete opatření, aby k dalším porušením zabezpečení nedocházelo.

Pokud hledáte odpovědi na jiné dotazy či podrobnější informace, naleznete je např. na www.uoou.cz.

www.mpo.cz/gdpr

www.uoou.cz/gdpr-strucne/ds-4843/p1=4843

Chráníme Vaše osobní údaje / GDPR pro živnostníky a malé podniky

Tímto vyhodnocujeme rizika spojená se zpracováním osobních údajů, přijímáme opatření k minimalizaci těchto rizik a seznamujeme dotčené osoby o zásadách zpracování osobních údajů dle nařízení GDPR.

- ANO Máme osobní údaje* zaměstnanců, dodavatelů a/nebo zákazníků
(*jméno, příjmení, adresa, e-mail, telefon a další nezbytné osobní údaje)
- ANO Máme pouze osobní údaje potřebné pro podnikání
- ANO Nepotřebné osobní údaje neshromažďujeme, pokud zákon nenařizuje uchování údajů, tak je mažeme
- ANO Nositele osobních údajů seznamujeme, že zpracováváme jejich osobní údaje a můžou u nás žádat o vysvětlení, o opravu, výmaz údajů či podat námitku proti jejich zpracování, nespokojení se můžou obrátit na dozorový orgán Úřad pro ochranu osobních údajů (www.uoou.cz, rubrika Poradna/Jak postupovat).
- ANO Nemáme citlivé údaje ani nevedeme zdravotní záznamy
(kromě posudků o zdravotním stavu a průceschopnosti zaměstnanců).
- ANO Předáváme osobní údaje pouze zaměstnancům a dodavatelům zavázaným mlčenlivostí
- ANO Máme osobní údaje v počítači a v telefonu chráněné heslem
- ANO Máme osobní údaje v zamčené místnosti
- ANO Máme důležité dokumenty s osobními údaji v normální uzamykatelné skříni
(pracovní smlouvy apod.)
- ANO Máme osobní údaje pouze pro svoje podnikání
(plnění smluv, objednávek apod.)
- ANO Máme osobní údaje pro plnění zákonných povinností
(vedení účetnictví, mezd apod.)
- ANO Máme osobní údaje pro ochranu svých zájmů
(správa pohledávek, soudní/správní/jiné řízení apod.)
- ANO Nikomu neoprávněnému nezpřístupňujeme osobní údaje
- ANO Nikomu neposíláme nevyžádanou poštu
- ANO Zaměstnanci ví, že musí chránit osobní údaje a jsou vázáni mlčenlivostí
- ANO Zaměstnanci ví, že osobní údaje nesmí zpřístupňovat neoprávněným osobám
- ANO Dodavatelé ví, že musí chránit osobní údaje a jsou vázáni mlčenlivostí
- ANO Dodavatelé ví, že osobní údaje nesmí zpřístupňovat neoprávněným osobám

Odpovědi ANO znamenají, že principálně vše děláme v souladu s nařízením GDPR.
Pokud ne, učiníme vždy opatření potřebná k odpovědi ANO, pak máme opět vše v pořádku.

Název firmy: _____

IČ: _____

Datum: _____

Podpis odpovědné osoby
(živnostník/ statutární zástupce)