

Jednoduchý návod, jak zacházet s osobními údaji

Zdroj: Úřad pro ochranu osobních údajů, www.uoou.cz

Jednoduchost a srozumitelnost budiž pochválena - i v případě aplikace GDPR.

Podívejte se na Desatero základních pravidel ochrany osobních údajů, využitelné malými správci údajů, živnostníky či menšími podniky, coby základní jednoduchý návod, jak zacházet s osobními údaji.

1. Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, **musí být legitimní** a nesmí být v rozporu s právními předpisy či morálkou.
2. Každé zpracování údajů musí být **založeno na některém ze základních důvodů** (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.
3. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr - **účel zpracování údajů**.
4. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být **vždy přiměřené účelu zpracování**.
5. Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít **jasný zákonný podklad**, takové zpracování nelze nahradit souhlasem se zpracováním údajů.
6. Správce i zpracovatel osobních údajů musí osobní údaje **patříčně zabezpečit** a chránit organizačními a technickými opatřeními – v míře odpovídající rizikovosti zpracování.
7. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno **férově, korektně a transparentně**. Informace o zpracování poskytované subjektu údajů musí být **zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci**.
8. Zpracování **nesmí nadměrně zasahovat do soukromí**. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.
9. Po naplnění účelu zpracování je dána povinnost osobní údaje **zlikvidovat**. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).
10. V rámci EU je v každé členské zemi zaručena unifikovaná ochrana osobních údajů, kterou stanoví obecné nařízení (GDPR). Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů.