

ZÁKLADNÉ POKYNY PRI PRÁCI S OSOBNÝMI ÚDAJMI

V rámci skupiny PPA sme sa dôkladne pripravili na nové pravidlá ochrany osobných údajov (známe ako GDPR). Nižšie nájdete zhrnutie základných pokynov a inštrukcií ako postupovať pri spracúvaní osobných údajov v našich spoločnostiach.



V skupine PPA pôsobí tzv. **zodpovedná osoba („DPO“)**, ktorého úlohou je monitorovať súlad s GDPR a internými predpismi. Je ním pán Marek Jurina (jurina@ppa.sk alebo 0905 723 076).

DPO je oprávnený udeľovať zamestnanom bližšie pokyny a inštrukcie v oblasti ochrany osobných údajov. Tieto **pokyny sú pre Vás záväzné**, pokiaľ riaditeľ dcérskej spoločnosti PPA, v ktorej pôsobíte, nerozhodne inak. Ak máte akékoľvek otázky týkajúce sa ochrany osobných údajov v rámci skupiny PPA, alebo zistíte akýkoľvek rozpor s pravidlami GDPR, alebo internými politikami, obráťte sa na DPO.



V skupine PPA sme prijali **dve kľúčové interné politiky** na zabezpečenie súladu s GDPR:

- Interná politika ochrany osobných údajov
- Bezpečnostná politika IT.

Politiky sú dostupné na: **www.ppa.sk/politiky**

Oboznámte sa s nimi bližšie, postupujte podľa nich v prípade otázok kontaktujte DPO.



Dokumenty a dátové súbory s obsahujúce osobné údaje zabezpečte tak, aby **nemohli byť skopírované, alebo odcudzené neoprávnenými osobami a tiež ich zabezpečte proti nožnej strate.**



Ak máte podozrenie alebo vedomosť že nastal tzv. **bezpečnostný incident** (strata, alebo odcudzenie osobných údajov, alebo akýkoľvek fyzické ohrozenie dát, alebo útok na výpočtovú techniku a komunikačnú techniku) – okamžite to nahláste DPO a v jeho neprítomnosti IT oddeleniu (p. Kostič – kostic@ppa.sk alebo 0905 972 745). Nahláste akýkoľvek bezpečnostný incident – aj malej závažnosti.



Pred odoslaním emailu sa vždy uistite, že ho zasielate **správnym adresátom**.



Neodpovedajte, neklikajte na odkazy a neotvárajte prílohy **podozrivých emailov**. Akúkoľvek podozrivú komunikáciu bezodkladne oznámte DPO a v jeho neprítomnosti IT oddeleniu (p. Kostič).



Ak zasielate veľké množstvo osobných údajov napr. v prílohe emailu, **prílohu emailu zabezpečte heslom**. Heslo pošlite adresátovi samostatne cez SMS. Osobné údaje uchovávané na prenosných dátových nosičoch (USB kľúče a disky) musia byť taktiež zabezpečené heslom.

V prípade otázok kontaktujte IT oddelenie alebo IT technika.



Pri akomkoľvek novom procese, rozhodnutí alebo projekte sa pro-aktívne zamýšľajte nad otázkou: **„Aký to bude mať dopad na ochranu súkromia?“** Požadujte zapojenie DPO ak si myslíte, že daný dopad existuje.

Ďakujeme Vám, že dodržiavaním týchto pravidiel budete chrániť svoje osobné údaje, osobné údaje Vašich kolegov a obchodných partnerov.