Bezpečnostní směrnice

Zabezpečení osobních údajů

M.G.P. spol. s r.o. (dále jen "organizace") v souladu s Nařízením 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 „Nařízení GDPR“) a v souladu se souvisejícími právními předpisy České republiky, je zpracovatelem osobních údajů fyzických osob.

1.1 Informační zabezpečení zpracování osobních údajů

1.1.1 Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být vždy přiměřené účelu zpracování.

1.1.2 Organizace musí osobní údaje patřičně zabezpečit a chránit organizačními a technickými opatřeními, a to v míře odpovídající rizikovosti zpracování.

1.1.3 Základním způsobem ochrany osobních údajů je omezení přístupů k osobním údajům jen pro osoby, které jej z důvodu zpracování údajů nezbytně potřebují (viz Politika přístupových oprávnění).

1.1.4 Údaje v informačních systémech organizace musí být všude tam, kde to dává smysl, šifrovány (viz Politika kryptografických opatření). Šifrovány nemusí být přenosy ve vnitřní síti.

1.1.5 Pro předání třetím osobám může organizace použít místo šifrování též pseudonymizaci.

1.1.6 Zaměstnancům je přísně zakázáno zpracovávat osobní data k jiným než organizací předepsaným účelům, nebo zpracovávat je ve větším než organizací předepsaném rozsahu, ukládat je mimo předepsaná úložiště, nebo je bez povolení organizace někam zasílat.

1.1.7 Zpracovávány mohou být pouze správné osobní údaje. Zjištěné chybné údaje musí být neprodleně opraveny, a pokud to není možné, pak vymazány.

1.2 Likvidace osobních údajů

1.2.1 Data obsahující osobní údaje, které již organizace nevyužívá k původnímu účelu, musí být v souladu s ustanovením Nařízení GDPR znepřístupněna, a to jakmile pomine účel, pro který byly osobní údaje zpracovávány, nebo jakmile uplyne lhůta určená ve Skartačním řádu, nebo na základě žádosti fyzických osob, kterých se příslušné osobní údaje týkají.

1.2.2 Vyhovujícím způsobem znepřístupnění je smazání dat, a pokud to technicky není možné provést (nelze např. mazat primární klíče v databázích), pak jejich pseudonymizace.

1.3 Monitorování osob provádějících zpracování osobních údajů

1.3.1 Monitorování osob musí probíhat jen v nezbytně nutném rozsahu, aby byla chráněna i oprávněná práva monitorovaných osob. Organizace vhodným způsobem informuje osoby, které jsou předmětem monitorování, a to vždy ještě před započetím monitorování.

1.3.2 Přístup k informacím získaným monitorováním mají pouze osoby k tomu pověřené vedením organizace.

1.4 Hlášení případů porušení zabezpečení osobních údajů dozorovému úřadu

1.4.1 Organizace je bez zbytečného odkladu, a pokud je to možné do 72 hodin od okamžiku, kdy bylo porušení zabezpečení zjištěno, povinna ohlásit ÚOOÚ porušení zabezpečení osobních údajů, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

1.4.2 Organizace dokumentuje veškeré případy porušení zabezpečení osobních údajů, a to tak, aby tato dokumentace umožnila ÚOOÚ ověření souladu s článkem 33 Nařízení GDPR.

1.4.3 Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob (a nejsou splněny vylučující podmínky uvedené v článku 34 Nařízení GDPR) oznámí organizace toto porušení bez zbytečného odkladu subjektům údajů.

1.4.4 K zajištění výše uvedených povinností pracovník IT neprodleně nahlásí osobě pověřené pro ochranu osobních údajů veškeré vzniklé bezpečnostní incidenty, které se týkají nebo mohou týkat osobních údajů.

1.4.5 Oznámení podle čl. 1.4.1 a 1.4.2 zasílá osoba pověřená pro ochranu osobních údajů, oznámení zasílané fyzickým osobám osoba pověřená pro ochranu osobních údajů projedná s vedením organizace.

1.5 Zajištění práv fyzických osob

1.5.1 Právo na přístup k osobním údajům – kopii zpracovávaných údajů vytvoří pracovník IT formou Printscreenu příslušných obrazovek příslušného informačního systému. Přitom je nutné dbát, aby screeny neobsahovaly údaje citlivé pro organizaci (např. obsahující obchodní tajemství organizace), nebo údaje týkající se jiných fyzických nebo právnických osob.

1.5.2 Právo na výmaz údajů – zajistí pracovník IT podle postupů uvedených v čl. 1.2.

1.5.3 Právo na omezení zpracování – bude zajištěno tak, že záznamy, které mají v informačním systému vyplněné pole „Omezeno do“, budou až do uvedeného data ze zpracování automaticky vyňaty.

1.5.4 Právo na přenositelnost údajů – zajistí pracovník IT tak, že provede export vybraného záznamu z databáze v textovém tvaru na CD nosič. Zároveň se vyjme záznam z dalšího zpracování (viz 1.5.3) a za 10 pracovních dnů poté se provede likvidace údajů podle postupů uvedených v čl. 1.2.