# 39.21. Porušení zabezpečení osobních údajů

http://www.guard7.cz/gdpr/poruseni-zabezpeceni-osobnich-udaju

GDPR – porušení zabezpečení osobních údajů

Porušení zabezpečení osobních údajů je jednání, které vede k

1. náhodnému nebo protiprávnímu zničení,
2. ztrátě,
3. změně,
4. neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

## Riziko

Při určování míry rizika porušení zabezpečení se bude vycházet:

1. z kategorie osobních údajů,
2. z charakteru porušení zabezpečení,
3. z počtu dotčených subjektů údajů,
4. zda došlo k porušení zabezpečení úmyslně či nedbalostně.
   Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu škodu – únik přihlašovacích údajů do elektronického bankovnictví apod.

## Ohlášení Úřadu pro ochranu osobních údajů

Pokud dojde k porušení zabezpečení osobních údajů, měl by správce zhodnotit, zdali nepředstavuje riziko pro práva a svobody fyzických

osob. Pokud ano, je nutné to ohlásit Úřadu pro ochranu osobních údajů, resp. oznámit subjektu údajů. To musí provést bez odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Pokud není ohlášení učiněno do 72 hodin, musí být současně s ním uvedeny důvody zpoždění.

V oznámení správce subjektu údajů popíše:

1. povahu porušení zabezpečení,
2. přijatá opatření,
3. pravděpodobné důsledky
4. kontaktní údaje na pověřence pro ochranu osobních údajů, byl-li ustaven.
   Pokud nastane porušení zabezpečení u zpracovatele, hlásí jej správci, pro kterého dotčené osobní údaje zpracovává.

## Ohlášení porušení subjektu údajů

Pokud porušení zabezpečení představuje vysoké riziko pro práva a svobody subjektu údajů, uvědomí o tom správce bez zbytečného odkladu dotčený subjekt údajů. V něm se uvede povaha porušení zabezpečení osobních údajů a informace o přijatých opatřeních.

Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

1. správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování,
2. správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví,
3. vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být

subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

4. Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil, nebo může rozhodnout, že je splněna některá z podmínek uvedených výše.

---

# Související legislativa

Zákon č. 101/2000 Sb., o ochraně osobních údajů.
Zákon č. 89/2012 Sb., občanský zákoník.
Zákon č. 127/2005 Sb. ,o elektronických komunikacích.
Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.
Nařízení GDPR.

(85) Není-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob. Jakmile se tedy správce o porušení zabezpečení osobních údajů dozví, měl by je bez zbytečného odkladu, a je-li to možné, do 72 hodin poté, co se o něm dozvěděl, ohlásit příslušnému dozorovému úřadu, ledaže může v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro

práva a svobody fyzických osob. Není-li toto ohlášení možné učinit do 72 hodin, měly by být spolu s ním uvedeny důvody zpoždění a informace mohou být poskytnuty postupně bez zbytečného dalšího prodlení