
Postup v prípade vzniku porušenia zabezpečenia osobných údajov (bezpečnostných incidentov) spracovaný v nadväznosti na Nariadenie európskeho parlamentu a Rady (EU) č. 2016/679 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe údajov (ďalej len GDPR)

Tyros Loading Systems SK, s.r.o. ako správca v zmysle ustanovenia článku 12 GDPR vytvoril túto metodiku obsahujúcu registráciu a ohlasovanie prípadov porušenia zabezpečenia osobných údajov orgánu dozoru a subjektu údajov podľa článku 33 a 34 GDPR.

1. Ochrana a zabezpečenie osobných údajov je zásadnou úlohou a cieľom GDPR a na správcovi je, aby vykonal také formálne, organizačné a technické zabezpečenia získaných osobných údajov, ktoré eliminujú možnosť poškodenia subjektov údajov únikom ich informácií nepovolaným osobám. Tento materiál slúži k tomu, že stanovuje pre prípad, že napriek prijatým opatreniam, k porušeniu ochrany a zabezpečenia osobných údajov výnimočne dôjde, postup, ktorý po zistení každého bezpečnostného incidentu musí správca vykonať.
2. Za porušenie zabezpečenia osobných údajov sú považované prípady, kedy dôjde k porušeniu zabezpečenia, ktoré vedie k náhodnému alebo protiprávnemu zničeniu, strate, zmene alebo neoprávnenému poskytnutiu alebo sprístupneniu prenášaných, uložených alebo inak spracovaných osobných údajov. Medzi prípady porušenia zabezpečenia osobných údajov patria tak priame útoky zvonka alebo zvnútra osobou správcu, teda prípady úmyselné i nedbanlivostné, ale aj rada menších prípadov, kedy správca stratí kontakt nad dátami, ktoré spravuje.
3. Akékoľvek porušenia zabezpečenia osobných údajov tak, ako sú špecifikované v odseku 2, s výnimkou tých prípadov, kedy správca po podrobnej analýze zhodnotí, že je nepravdepodobné, že by také konkrétne porušenie zabezpečenia osobných údajov malo za následok vysoké riziko pre práva a slobody subjektu údajov, správca bezodkladne, najneskôr do 72 hodín od ich zistenia ohlásí dozorovému orgánu, teda Úradu na ochranu osobných údajov. Pri určovaní miery rizika porušenia zabezpečenia osobných údajov sa bude vychádzať z kategórie osobných údajov, ktoré boli porušením zabezpečenia dotknuté, charakteru porušenia a počtu dotknutých subjektov údajov. Ďalším rozhodným prvkom pre stanovenie miery rizika je okolnosť, či k porušeniu zabezpečenia osobných údajov došlo úmyselne alebo z nedbanlivosti. Porušenie zabezpečenia osobných údajov je vždy nutné vykonať komplexne a ešte len zistená miera rizika určí povinnosť prípadne oznámiť porušenie zabezpečenia dozorovému orgánu.
4. Ak správca vyhodnotí, že nastal prípad spojovaný GDPR s povinnosťou oznámiť porušenie zabezpečenia osobných údajov dozorovému orgánu, ohlásí mu ho. Ohlásenie musí obsahovať tieto údaje:
 - popis povahy daného prípadu porušenia zabezpečenia osobných údajov vrátane, ak je to možné, špecifikácie kategórií a približného počtu dotknutých subjektov údajov a kategórií a približného počtu dotknutých osobných údajov,
 - meno a kontaktné údaje na kontaktné mieste, ktoré môže poskytnúť bližšie informácie o danom prípade,
 - popis pravdepodobných dôsledkov porušenia zabezpečenia osobných údajov,

- popis opatrení, ktoré správca prijal alebo k prijatiu navrhol s cieľom vyriešiť porušenie zabezpečenia osobných údajov, vrátane prípadných opatrení na zmiernenie možných nepriaznivých dôsledkov.
5. Správca má povinnosť dokumentovať všetky prípady porušenia zabezpečenia osobných údajov a vždy uvedie všetky skutočnosti, ktoré sa týkajú daného prípadu porušenia, jeho účinky a prijaté nápravné opatrenia.
 6. Ak správca zistí, že je pravdepodobné, že konkrétny prípad porušenia zabezpečenia osobných údajov bude mať za následok vysoké riziko pre práva a slobody subjektov údajov, oznámi správca toto porušenie bez zbytočného odkladu dotknutému subjektu údajov.
 7. V oznámení podľa bodu 6 správca zrozumiteľne popíše subjektu údajov povahu porušenia zabezpečenia osobných údajov a uvedie v ňom aspoň tieto nasledovné informácie:
 - meno a kontaktné údaje na kontaktné miesto, ktoré môže poskytnúť bližšie informácie o danom prípade,
 - popis pravdepodobných dôsledkov porušenia zabezpečenia osobných údajov,
 - popis opatrení, ktoré správca prijal alebo k prijatiu navrhol s cieľom vyriešiť porušenie zabezpečenia osobných údajov, vrátane prípadných opatrení na zmiernenie možných nepriaznivých dôsledkov.
 8. Oznámenie podľa bodu 7 sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok:
 - správca zaviedol náležité technické a organizačné ochranné opatrenia a tieto opatrenia boli použité pri osobných údajoch dotknutých porušením zabezpečenia osobných údajov, najmä také, ktoré robia tieto údaje nezrozumiteľnými pre kohokoľvek, kto nie je oprávnený mať k nim prístup, ako je napríklad šifrovanie,
 - správca prijal následné opatrenia, ktoré zaistia, že vysoké riziko pre práva a slobody subjektov údajov podľa bodu 6 sa už pravdepodobne neprejaví,
 - vyžadovalo by to neprimerané úsilie. V takomto prípade musí byť dotknutý subjekt údajov informovaný rovnako účinným oznámením pomocou verejného oznámenia alebo podobného opatrenia.
 9. Vedúci pracovník správcu v prípade každého zistenia porušenia zabezpečenia osobných údajov prejedná tento prípad vo všetkých súvislostiach so zamestnancom správcu, ktorý je také porušenie zodpovedný alebo ktorý má na starosti oblasť, v ktorej k porušeniu zabezpečenia osobných údajov došlo a vyvodí voči nemu zodpovedajúce dôsledky.
 10. Správca vedie evidenciu všetkých zistených prípadov porušenia zabezpečenia osobných údajov v rozsahu podľa prílohy k tomuto dokumentu.

Príloha: evidenčný list prípadov porušenia zabezpečenia osobných údajov

Vo Vrbovom, dňa 01. 05. 2018

Podpis štatutárneho zástupcu správcu:

Tyros Loading Systems SK s.r.o.
Šteruská cesta 21
922 03 Vrbové
Tel.: +421 33/774 87 95, Fax: +421 33/773 1571
IČO: 35 258 598 DIČ: 2021787834
IČ DPH: SK2021787834

