Postup při vzniku případů porušení zabezpečení osobních údajů (bezpečnostních incidentů) zpracovaný v návaznosti na Nařízení evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu údajů (dále jen GDPR)

Tyros Loading Systems CZ s.r.o. jakožto správce ve smyslu ustanovení článku 12 GDPR vytvořil tuto metodiku popisující registraci a ohlašování případů porušení zabezpečení osobních údajů dozorovému orgánu a subjektu údajů dle článků 33 a 34 GDPR.

1. Ochrana a zabezpečení osobních údajů je zásadním úkolem a cílem GDPR a na správci je, aby provedl taková formální, organizační a technická zabezpečení získaných osobních údajů, která eliminují možnost poškození subjektů údajů únikem jejich informací nepovolaným osobám. Tento materiál slouží k tomu, že stanovuje pro případ, že přes přijatá opatření k porušení ochrany a zabezpečení osobních údajů výjimečně dojde, postup, který po zjištění každého bezpečnostního incidentu musí správce provést.
2. Za porušení zabezpečení osobních údajů jsou považovány případy, kdy dojde k porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Do případů porušení zabezpečení osobních údajů spadají jak přímé útoky zvenčí nebo zevnitř osoby správce, tedy případy úmyslné i nedbalostní, ale i řada drobnějších případů, kdy správce ztratí kontakt nad daty, která spravuje.
3. Jakékoliv porušení zabezpečení osobních údajů tak, jak jsou specifikovány v odstavci 2, s výjimkou těch případů, kdy správce po podrobné analýze shledá, že je nepravděpodobné, že by takové konkrétní porušení zabezpečení osobních údajů mělo za následek vysoké riziko pro práva a svobody subjektu údajů, správce bezodkladně, nejpozději do 72 hodin od jejich zjištění ohlásí dozorovému orgánu, tedy Úřadu na ochranu osobních údajů. Při určování míry rizika porušení zabezpečení osobních údajů se bude vycházet z kategorie osobních údajů, které byly porušením zabezpečení dotčeny, charakteru porušení a počtem dotčených subjektů údajů. Dalším rozhodným prvkem pro stanovení míry rizika je okolnost, zda k porušení zabezpečení osobních údajů došlo úmyslně či z nedbalosti. Porušení zabezpečení osobních údajů je vždy nutno provést komplexně a teprve zjištěná míra rizika určí povinnost případně oznámit porušení zabezpečení dozorovému orgánu.
4. Vyhodnotí-li správce, že nastal případ spojovaný GDPR s povinností oznámit porušení zabezpečení osobních údajů dozorovému orgánu, ohlásí mu ho. Ohlášení musí obsahovat tyto údaje:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, specifikace kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného počtu dotčených osobních údajů,
- jméno a kontaktní údaje na kontaktní místo, které může poskytnout bližší informace o daném případu,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, které správce přijal nebo k přijetí navrhl, s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření na zmírnění možných nepříznivých důsledků,

5. Správce má za povinnost dokumentovat všechny případy porušení zabezpečení osobních údajů a vždy uvede všechny skutečnosti, které se týkají daného případu porušení, jeho účinky a přijatá nápravná opatření.
6. Pokud správce zjistí, že je pravděpodobné, konkrétní případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody subjektu údajů, oznámí správce toto porušení bez zbytečného odkladu dotčenému subjektu údajů.

7. V oznámení podle bodu 6 správce srozumitelně popíše subjektu údajů povahu porušení zabezpečení osobních údajů a uvede v něm alespoň dále tyto informace:
- jméno a kontaktní údaje na kontaktní místo, které může poskytnout bližší informace o daném případu,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, které správce přijal nebo k přijetí navrhl, s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření na zmírnění možných nepříznivých důsledků.
8. Oznámení podle bodu 7 se nevyžaduje, je -li splněna kterákoliv z těchto podmínek
- 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 kohokoliv, kdo není oprávněn k nim mít přístup, jako je například šifrování,
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle bodu 6 se již pravděpodobně neprojeví,
- vyžadovalo-li by to nepřiměřené úsilí. V takovém případě musí být dotčený subjekt údajů informován stejně účinným oznámením pomocí veřejného oznámení nebo podobného opatření.
9. Vedoucí pracovník správce v případě každého zjištění porušení zabezpečení osobních údajů projedná tento případ ve všech souvislostech se zaměstnancem správce, který je za takové porušení odpovědný nebo který má na starosti oblast, ve které k porušení zabezpečení osobních údajů došlo a vyvodí proti němu odpovídající důsledky.
10. Správce vede evidenci všech zjištěných případů porušení zabezpečení osobních údajů v rozsahu dle přílohy k tomuto dokumentu.

Příloha: evidenční list případů porušení zabezpečení osobních údajů

V Praze dne:3.5.2018

Podpis statutárního zástupce správce: