Č. j. MSPUČ 133/2019

Směrnice pro postup při porušení bezpečnosti osobních údajů

1. Oprávněné osoby jsou povinni v případě zjištění porušení zabezpečení osobních údajů, nebo nabytí podezření neprodleně informovat v případě zaměstnanců svého nadřízeného a v případě členů orgánů obce starostu, nebo místostarostu, který následně informuje pověřence.
2. Pověřenec na základě hlášení o porušení zabezpečení osobních údajů v součinnosti s příslušným vedoucím zaměstnancem:
    a) Vyhodnotí zdroje porušení (interní, externí atd.),
    b) Vyhodnotí základní informace o narušení a rozhodne o klasifikaci narušení, tj. zda se jedná o bezpečnostní událost (situace, kdy mohlo dojít k selhání některého z bezpečnostních opatření a tím mohlo dojít k porušení zabezpečení ochrany osobních údajů) nebo bezpečnostní incident (situace, kdy došlo k selhání některého z bezpečnostních opatření a tím došlo k porušení zabezpečení ochrany osobních údajů).
3. Pokud je informace vyhodnocena jako **bezpečnostní událost**, provede pověřenec v rámci dalšího šetření následující kroky:
    a) Prověří v záznamech, zda se jedná o nahodilou událost, nebo se jedná o událost, která se opakuje
    b) Vypracuje návrh na opatření k nápravě,
    c) Návrh na opatření k nápravě předá starostovi obce
4. Pokud je informace vyhodnocena jako **bezpečnostní incident**, pověřenec přizve další osoby, které jsou kompetentní pro jeho posouzení a provedou se následující činnosti:
    a) Pokud je možné, provedou odpovědní zaměstnanci okamžitou nápravu (zastavení provozu, zablokování přístupových oprávnění atd.),
    b) Identifikace kategorie porušení
        - Porušení důvěrnosti
        - Porušení dostupnosti
        - Porušení integrity
    c) Identifikace typů osobních údajů, u kterých došlo k porušení bezpečnosti
    d) Stanovení přibližného objemu údajů, u kterých došlo k porušení bezpečnosti
    e) Identifikace pravděpodobného zdroje úniku, či případného porušení zabezpečení osobních údajů
    f) Popis pravděpodobných důsledků dopadů na subjekty údajů
    g) Vyhodnocení rizika dopadů na práva a svobody subjektů údajů:
        - Bez rizika
        - S rizikem
        - S vysokým rizikem

5. Po vyhodnocení rizika pověřenec informuje starostu a společně s ním přijme rozhodnutí (o povinnosti ohlášení, nebo oznámení) a v případě vyhodnocení:

a) Rizika – provede ohlášení ÚOOÚ, (bez zbytečného odkladu do 72 hodin od zjištění bezpečnostního incidentu)
b) Vysokého rizika – provede ohlášení ÚOOÚ a oznámení subjektům údajů, (bez zbytečného odkladu).

6. Dále pověřenec společně s dalšími odpovědnými zaměstnanci vypracuje návrh a odpovědní vedoucí zaměstnanci přijmou a neprodleně zrealizují prvotní možná nápravná opatření ke snížení dopadů na práva subjektů údajů, nebo k eliminaci příčiny porušení bezpečnosti osobních údajů.
7. Pověřenec připraví a zpracuje hlášení v souladu s čl. 33 odst. 3 písm. a) až d) nebo s čl. 33 odst. 3 písm. b) až d) obecného nařízení, vždy podle úrovně vyhodnoceného rizika, které po schválení starostou odešle příslušným subjektům (ÚOOÚ, případně subjektů, údajů).
8. Pověřenec v součinnosti s odpovědnými vedoucími zaměstnanci po odeslání hlášení provede:
    a) Další došetřování incidentu na základě návrhů uvedených v hlášení ÚOOÚ
    b) Vypracuje návrh na přijetí dalších nápravných opatření
    c) Kontrolu účinnosti přijatých opatření
9. Pověřenec společně s dalšími odpovědnými zaměstnanci zpracovává dokumentaci týkající se porušení zabezpečení osobních údajů. Dokumentace musí obsahovat:
    a) Veškeré skutečnosti, které se týkají příslušného porušení
    b) Dopady porušení a
    c) Přijatá nápravná opatření
10. Dokumentace o porušení zabezpečení osobních údajů musí ÚOOÚ umožnit ověření v souladu s obecným nařízením.

V Přestavlkách u Čerčan dne 2. 1. 2019