**10. Vzorová dokumentace případů porušení zabezpečení a vzorové ohlášení porušení zabezpečení**

Jako správce osobních údajů vést dokumentaci všech případů porušení zabezpečení osobních údajů a některá porušení oznámit Úřadu pro ochranu osobních údajů. V této části najdete vzory, které Vám při plnění těchto povinností pomohou.

**Co je porušení zabezpečení osobních údajů?**

Může se jednat o celou řadu situací, např.:

* do zdravotnické dokumentace nahlédne neoprávněná osoba, např. jiný pacient, uklízečka apod.
* počítač se zdravotnickou dokumentací se rozbije a data v něm uložená budou zničena
* Váš výpočetní systém bude napaden hackery, jimž se podaří prolomit veškerou ochranu a zmocnit se všech údajů o Vašich pacientech,
* ztratíte mobilní telefon, v němž budou uloženy kontakty na Vaše pacienty i Vaše objednací diář,
* při povodni bude zničen Váš archiv zdravotnické dokumentace,
* do telefonu sdělíte údaj o zdravotním stavu osobě, která se vydávala za Vašeho pacienta,
* Váš počítač začne sám od sebe rozesílat údaje o Vašich pacientech všem osobám, jejich elektronické adresy jsou uloženy ve Vašem poštovním programu,
* lidé v čekárně slyšeli diagnózu, kterou sděloval lékař pacientovi v ordinaci,
* zdravotní sestra přečetla pacientovi výsledky jeho krevních testů v čekárně před ostatními pacienty apod.

Pokud k nějakému podobnému případu dojde, je třeba jej především zaznamenat. Záznam musí obsahovat

* **popis případu**. To je v podstatě vylíčení toho, k čemu došlo. Např.: *„Zaměstnanec správce v rozporu se svými povinnostmi po skončení ordinační doby zanechal na stole v ordinaci volně položené zdravotní karty 2 pacientů, ordinaci opustil a zamkl.“*
* **účinky porušení zabezpečení**. Zde je třeba stručně popsat, jaký dopad na osobní údaje incident měl. Např.: „*Jiný zaměstnanec správce při úklidu ordinace předmětné zdravotní karty společně s dalšími listinami považoval za odpad a vložil je do nádoby na tříděný odpad, která se nachází ve zdravotnickém zařízení. Druhý den byly všechny karty nalezeny a vráceny do kartotéky.“*
* **přijatá opatření**. Je třeba stručně uvést, co jste udělali pro to, aby k podobnému problému již nedošlo. Např.: *„Zaměstnanci správce byli opakovaně poučeni o pravidlech nakládání se zdravotnickou dokumentací.“*
* **oznámeno ÚOOÚ**. Sem zapíšete poznámku, zda jste incident oznámili Úřadu pro ochranu osobních údajů (ANO), nebo neoznámili (NE) s krátkým zdůvodněním. Např.: *„NE. Do zdravotnické dokumentace nikdo nenahlížel, karty byly nepoškozené nalezeny, neopustily přitom zdravotnické zařízení. Riziko pro práva a svobody fyzických osob bylo zanedbatelné.“*

**Oznámení porušení zabezpečení ÚOOÚ**

Zatímco dokumentaci musíte vést o každém porušení zabezpečení, oznamovat Úřadu pro ochranu osobních údajů je třeba jen takové případy, které představují reálné riziko pro práva a svobody fyzických osob. K posouzení, zda porušení zabezpečení je rizikové, můžete využít tabulku č. 3. Pokud v některém řádku této tabulky nacházíte hodnotu 20 a vyšší, jde o zpracování s rizikem.

Tak např. v buňce C5 je hodnota 40. To znamená, že když ke zdravotnické dokumentaci pacienta získá přístup neoprávněná osoba, je to riziko pro právo na soukromí dotčeného pacienta. Ohrožení práv jednoho člověka však není nikdy tak závažné, aby bylo nutno je oznamovat ÚOOÚ. Oznámení bude nutné, pokud jsou reálnému riziku (hodnota 20 a vyšší v tabulce č. 3) vystaveni alespoň 2 živí lidé; takový incident bude třeba oznámit ÚOOÚ.

**Obsah a lhůta pro oznámení oznámení**

Obsahové náležitosti oznámení najdete v připojeném vzoru. Oznámení musíte učinit do 72 hodin od doby, kdy se o porušení bezpečnosti dozvíte. Pokud byste oznámení podávali později, je třeba toto zpoždění zdůvodnit.

**Oznámení porušení zabezpečení subjektům údajů**

Protože jste ambulantní poskytovatel, který nezpracovává osobní údaje v takovém rozsahu, aby to mohlo znamenat vysoké riziko pro práva a svobody fyzických osob, nemusíte porušení zabezpečení oznamovat subjektům údajů (tedy pacientům, zaměstnancům apod.).

**Dokumentace všech případů porušení zabezpečení osobních údajů**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **datum** | **popis případu** | **účinky porušení zabezpečení** | **přijatá opatření** | **Oznámeno ÚOOÚ** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Úřad pro ochranu osobních údajů

Pplk. Sochora 27

170 00 Praha 7

**Ohlášení porušení zabezpečení osobních údajů**

1. **Správce osobních údajů**

……………………………………………… *(jméno a příjmení, nebo obchodní firma)*

……………………………………………… *(identifikační číslo osoby – IČO)*

……………………………………………… *(sídlo)*

……………………………………………… *(elektronická adresa)*

1. **Datum a popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů**
2. **Jméno a kontaktní údaje osoby, která může poskytnout bližší informace**
3. **Popis pravděpodobných důsledků porušení zabezpečení osobních údajů**
4. **Popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů**

V ………... dne …………. ……………………………………….

podpis správce nebo osoby zastupující správce