

DOKUMENTACE PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Základní a Mateřská škola Chodouny, se sídlem Chodouny 119, 411 71 Chodouny, jakožto správce osobních údajů (dále jen „správce“), tímto dokumentem stanovuje pravidla postupu při porušení zabezpečení osobních údajů (bezpečnostní incident) a upravuje způsob dokumentování těchto bezpečnostních incidentů v souladu s články 32 – 34 obecného nařízení Evropského parlamentu a Rady č. 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení GDPR“).

1. V souladu s článkem 32 obecného nařízení GDPR **zavedl** správce osobních údajů, s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, **technická a organizační opatření**, aby zajistil úroveň zabezpečení osobních údajů odpovídající danému riziku. Technická a organizační opatření jsou popsána ve vnitřních předpisech správce, zejména pak ve „Směrnici pro ochranu osobních údajů“.
2. Porušením zabezpečené osobních údajů se dle článku 4 odst. 12 obecného nařízení GDPR rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Porušením zabezpečení (bezpečnostní incident) může být například kybernetický útok, narušení systému, v jehož rámci dochází ke zpracování osobních údajů, ztráta osobních složek zaměstnanců, úmyslné či nedbalostní poskytnutí osobních údajů zaměstnancem neoprávněně třetí osobě, nechtěné zveřejnění osobních údajů nebo neautorizovaný přístup k nim, nežádoucí či neautorizovaná změna osobních údajů, ztráta šifrovaného klíče, nevratná likvidace dat aniž by se jednalo o plnění povinnosti správce, zničení evidence v důsledku povodní, požáru atp.
3. Správce **ohlásí porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů**, představuje-li porušení riziko pro práva a svobody fyzických osob. Ohlášení provede správce bez zbytečného 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 tohoto zpoždění. Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Včasné ohlášení Úřadu pro ochranu osobních údajů může snížit případné riziko. Úřad může doporučit správci, jak incident řešit anebo využít pravomocí podle článku 58 obecného nařízení GDPR. Ohlášení obsahuje informace v rozsahu dle čl. 33 obecného nařízení GDPR. Vzor ohlášení je přílohou č. 1 této dokumentace.
4. Ohlašovány **nemusí být drobná porušení zabezpečení (drobné bezpečnostní incidenty)**, která ve svém důsledku pravděpodobně nepředstavují riziko pro práva subjektů údajů (např. únik šifrovaných nebo pseudonymizovaných osobních údajů, ztráta

služebního mobilu zaměstnance s přístupem k pracovnímu e-mailu pokud má správce bezpečnostní nástroj pro kontrolu mobilních zařízení a mobilní telefon ihned dálkově zablokuje atp.).

5. V případě, že porušení zabezpečení **pravděpodobně představuje vysoké riziko** pro práva subjektů údajů, **oznámí** správce bezpečnostní incident bez zbytečného odkladu **dotčeným subjektům údajů**, a to srozumitelně za použití jasných a jednoduchých jazykových prostředků. Oznámení obsahuje informace v rozsahu dle čl. 34 obecného nařízení GDPR. Vzor oznámení je přílohou č. 2 této dokumentace. Vysoké riziko pro práva subjektů údajů je pravděpodobné zejména v případech, kdy subjekty údajů v důsledku bezpečnostního incidentu mohou i potenciálně dojít k jakékoliv újmě z hlediska psychiky, cti, pověsti, zapříčinění diskriminace či újmy na majetku (např. uniknou-li citlivé či zneužitelné údaje, nebo jsou-li zničeny důležité osobní údaje bez zálohy). Vyžaduje-li oznámení bezpečnostního incidentu nepřiměřené úsilí, subjekty údajů jsou informovány veřejným oznámením nebo podobným opatřením (např. na webových stránkách správce). **Oznámení dotčeným subjektům údajů se nevyžaduje**, pokud správce zavedl preventivní nebo následná opatření, která zajistí, že vysoké riziko se pravděpodobně neprojeví (např. šifrování nebo znehodnocení uniklých osobních údajů).
6. Správce **dokumentuje** všechny případy porušení zabezpečení bez ohledu na to, zda bezpečnostní incident musí být ohlášen Úřadu pro ochranu osobních údajů nebo oznámen dotčeným subjektům údajů. Dokumentace obsahuje popis porušení zabezpečení osobních údajů, popis pravděpodobných důsledků (jeho účinky) a přijatá nápravná opatření, a je vedena tak, aby umožnila Úřadu pro ochranu osobních údajů ověřit soulad postupu s právní úpravou. Vzor tabulky pro dokumentování případů porušení zabezpečení je přílohou č. 3 této dokumentace.
7. Správce určí jednoho nebo několik odpovědných zaměstnanců, kteří posuzují povahu a okolnosti porušení zabezpečení. V případě zjištění porušení zabezpečení zaměstnanec neprodleně informuje ředitele školy, popř. pověřenou osobu, která ho v době nepřítomnosti zastupuje. Ředitel školy, pověřená osoba, popř. i jiný odpovědný zaměstnanec, kontaktuje pověřence pro ochranu osobních údajů. **(upravit postup dle konkrétních zvyklostí školy)**. Ředitel školy, resp. pověřená osoba rozhodne o tom, zda porušení zabezpečení ohlásí Úřadu pro ochranu osobních údajů a/nebo oznámí dotčeným subjektům údajů.
8. Při porušení zabezpečení je třeba zjišťovat konkrétní skutečnosti, tzn., co se skutečně stalo, kdy a jak k porušení došlo, jaké osobní údaje (kategorie osobních údajů, množství, rozsah) byly ohroženy anebo mohly uniknout či jakého množství subjektů údajů se porušení týká.
9. Při posuzování je třeba zohlednit, zda porušení zabezpečení představuje riziko pro práva a svobody fyzických osob – poměřovat dopad na subjekty údajů ve vztahu ke ztrátě kontroly nad osobními údaji, škodě na reputaci, možnosti omezení jejich práv, zapříčinění diskriminace, majetkové újmy atp. s přihlédnutím k počtu dotčených subjektů údajů, který je ale jenom podpůrným elementem, jelikož i bezpečnostní incident zahrnující pouze jeden subjekt údajů může být vysoce rizikový.

10. Správce přijme adekvátní nápravná opatření dle konkrétní situace a vše zdokumentuje (viz. bod č. 6).
11. Správce po získání všech relevantních informací, popř. získání výstupu z šetření Úřadu pro ochranu osobních údajů, provede vyhodnocení porušení zabezpečení a navrhne další bezpečnostní opatření (v oblasti fyzické, objektové, technické, personální či administrativní bezpečnosti) pro zvýšení ochrany a zamezení porušení zabezpečení do budoucna.

Formuláře

Součástí tohoto dokumentu jsou formuláře, které správce použije pro Ohlášení porušení zabezpečení Úřadu pro ochranu osobních údajů, Oznámení porušení zabezpečení osobních údajů subjektu údajů a Dokumentování případů porušení zabezpečení osobních údajů (bezpečnostních incidentů). Jedná se o tyto formuláře:

- Příloha č. 1 - Ohlášení případu porušení zabezpečení osobních údajů dle článku 33 obecného nařízení GDPR
- Příloha č. 2 – Oznámení případu porušení zabezpečení osobních údajů subjektu údajů dle článku 34 obecného nařízení GDPR
- Příloha č. 3 – Dokumentování případů porušení zabezpečení osobních údajů (bezpečnostních incidentů).

Vdne2019

.....
ředitelka školy

**Ohlášení případu porušení zabezpečení osobních údajů
dle článku 33 obecného nařízení GDPR**

Správce osobních údajů: **Základní a Mateřská škola Chodouny, Chodouny 119, 411 71 Chodouny**

Kontaktní údaje:**doplnit**

Pověřenec pro ochranu osobních údajů: Ing. Jana Chládková, kontaktní údaje: 739 605 925, chladkovagdpr@gmail.com

Popis porušení zabezpečení	
Datum vzniku	
Popis daného případu	
Kategorie dotčených subjektů údajů	<i>vyplňuje se, jen pokud je to možné</i>
Přibližný počet dotčených subjektů údajů	<i>vyplňuje se, jen pokud je to možné</i>
Kategorie dotčených záznamů osobních údajů	<i>vyplňuje se, jen pokud je to možné</i>
Přibližné množství dotčených záznamů osobních údajů	<i>vyplňuje se, jen pokud je to možné</i>
Popis pravděpodobných důsledků porušení zabezpečení	
Důsledek 1	
Důsledek 2	
Důsledek 3	
Popis přijatých nápravných opatření k řešení porušení zabezpečení včetně opatření ke zmírnění možných nepříznivých dopadů	
Opatření 1	
Opatření 2	
Opatření 3	
Popis důvodů zpoždění ohlášení (lhůta - do 72 hodin od zjištění porušení zabezpečení)	
Důvod 1	
Důvod 2	
Důvod 3	

Oznámení případu porušení zabezpečení osobních údajů subjektu údajů dle článku 34 obecného nařízení

Základní a Mateřská škola Chodouny
Chodouny 119
411 71 Chodouny

Adresát (jméno, příjmení, kontakt pro zaslání informace)

Vážená paní/Vážený pane,

informujeme Vás, že dne došlo v (název školy) v rámci zpracování Vašich osobních údajů k bezpečnostnímu incidentu, při kterém došlo ke.....(*popsat incidentu, jeho povahy a rozsahu*).

Z informací, které máme v současné chvíli k dispozici, lze předpokládat, že důsledky porušení zabezpečení (bezpečnostního incidentu) budou.....(*popsat důsledky, které pravděpodobně nastanou pro subjekty údajů a jejich osobní údaje*).

Pro zamezení či zmírnění negativních dopadů na Vaši osobu a osobní údaje a k celkovému vyřešení tohoto incidentu, jsme přijali několik nápravných opatření. Jedná se(*popíší se konkrétní přijatá nápravná opatření k řešení bezpečnostního incidentu včetně opatření ke zmírnění možných nepříznivých dopadů*).

V případě jakýchkoliv dotazů a bližšího vysvětlení této situace se můžete obrátit na našeho pověřence pro ochranu osobních údajů*jméno, příjmení a kontaktní údaje*.

S pozdravem

Jméno a příjmení

ředitelka školy

Základní a Mateřská škola Chodouny**Tabulka: Dokumentování případů porušení zabezpečení osobních údajů (bezpečnostních incidentů).**

Datum	Popis porušení zabezpečení osobních údajů	Kategorie a přibližný počet dotčených subjektů údajů	Kategorie a přibližné množství dotčených záznamů osobních údajů	Popis pravděpodobných důsledků	Přijatá nápravná opatření
	<i>povinný údaj</i> <i>Správce zde uvede skutečnosti, které se týkají daného porušení. Správce zaznamenává i takové případy porušení, které se neohlašují dozorovému úřadu, jelikož nepředstavují rizika pro práva a svobody fyzických osob.</i> <i>Zaznamenává se, kdy k porušení došlo, kdy, jak a kým bylo zjištěno, k jakému porušení došlo, jaké údaje či informace byly ohroženy anebo mohly uniknout. Dále se zaznamenávají další podstatné okolnosti dle</i>	<i>jen je-li to možné</i>	<i>jen je-li to možné</i>	<i>povinný údaj</i> <i>Správce zde uvede a popíše důsledky porušení zabezpečení, včetně situace, že porušení zabezpečení žádné důsledky nemělo, jelikož mu bylo včas zabráněno. Pokud porušení důsledky mělo, uvede se, zda došlo k úniku údajů, podrobně se rozepíše, jaké údaje unikly, v jakém množství, zda se jednalo o zvláštní kategorii osobních údajů.</i>	<i>povinný údaj</i> <i>Správce uvede konkrétní opatření, která vedla k nápravě a k zamezení opakování podobného bezpečnostního incidentu v budoucnu. Konkrétní přijatá opatření podrobně rozepíše. Správce dále uvede, zda došlo k ohlášení porušení zabezpečení dozorovému úřadu – kdy, komu, jakým způsobem a kdo ohlášení provedl. Správce rovněž uvede zda došlo k oznámení porušení zabezpečení i dotčeným subjektům údajů.</i>

	<i>konkrétní situace porušení zabezpečení osobních údajů.</i>				

