Č.j. SŠŘ 105/2019

STŘEDNÍ ŠKOLA ŘEMESLNÁ
A ZÁKLADNÍ ŠKOLA, SOBĚSLAV, WILSONOVA 405

S M Ě R N I C E
O POSTUPECH ORGANIZACE V PŘÍPADĚ BEZPEČNOSTNÍCH INCIDENTŮ A PORUŠENÍ OCHRANY OSOBNÍCH ÚDAJŮ

1. Působnost směrnice

Tato směrnice popisuje postupy, které zvolí organizace jako správce popř. i jako zpracovatel osobních údajů (dále jen *Správce* resp. *Zpracovatel)* v případě, že u ní nastane bezpečnostní incident nebo porušení zabezpečení osobních údajů. Vymezuje, zda a kdy vznikne správci osobních údajů ohlašovací povinnost dozorovému úřadu a oznamovací povinnost subjektu osobních údajů, a uvádí, jaké informace je nutno předat, včetně vymezení času. Dále směrnice řeší dokumentaci bezpečnostních incidentů a porušení ochrany osobních údajů a zmiňuje úlohu pověřence pro ochranu osobních údajů.

2. Definice:

a. **Bezpečnostní incident** – situace, při které došlo k ohrožení bezpečnosti osobních údajů nebo k porušení pravidel. Bezpečnostní incident vzniká v důsledku selhání nebo nedodržení bezpečnostních opatření nebo porušení bezpečnostní politiky.[1] Při bezpečnostním incidentu může dojít k ohrožení, ztrátě, odcizení, zneužití nebo změně dat nebo informací.

b. **Porušení zabezpečení osobních údajů** – druh bezpečnostního incidentu. Jde o porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupněných přenášených, uložených nebo jinak zpracovávaných osobních údajů.

c. **Typy porušení zabezpečení osobních údajů:**

- porušení důvěrnosti – v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů.
- porušení dostupnosti – v případě neoprávněné nebo náhodné ztráty přístupu nebo zničení osobních údajů.
- porušení integrity – v případě neoprávněného nebo náhodného pozměnění osobních údajů.

d. **Zničení osobních údajů** – osobní údaje už neexistují vůbec nebo existují pouze v podobě, kdy nejsou správci k užitku.

e. **Poškození osobních údajů** – osobní údaje byly pozměněny nebo nejsou kompletní.

f. **Ztráta osobních údajů** – osobní údaje mohou stále existovat, ale správce ztratil kontrolu nad nimi nebo přístup k nim, nebo už je nemá v držení.

g. **Neoprávněné nebo protiprávní zpracování osobních údajů** – zpřístupnění osobních údajů (nebo přístup k nim) příjemcům, kteří nemají oprávnění data získat (nebo mít k nim přístup), nebo jakoukoliv jinou formu zpracování, která je v rozporu s Obecným nařízením[2].

3. Činnost Správce při bezpečnostním incidentu

Odpovědné osoby pověřené řešením incidentů, zjišťováním výskytu porušení a posuzováním rizika jsou: vedoucí provozně-ekonomického úseku, ICT technik, metodik a koordinátor ICT, . V případě, že Správce zjistí, že došlo k bezpečnostnímu incidentu, neprodleně provede šetření, zda nedošlo k porušení zabezpečení osobních údajů. Bezpečnostním incidentem mohou být např. tyto události: krádež, vykradení, vloupání, útok, neoprávněný přístup k informacím nebo datům, neoprávněné použití informací, neoprávněný vstup do budovy nebo do systému, smazání dat, selhání infrastruktury nebo připojení, selhání serveru, databáze nebo aplikace, hackerský útok, průnik do systému dat, virový útok, útok vyděračským softwarem (ransomware), přírodní katastrofa, falšování webové stránky (spoofing),

[1] Jako bezpečnostní incident může být vyhodnocený i pouhý neúspěšný pokus o zcizení nebo jiné znehodnocení informací.

[2] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

pokus o zcizení informací apod. Pokud nedošlo k porušení bezpečnosti osobních údajů, Správce zdokumentuje bezpečnostní incident pro případ, že by se toto porušení prokázalo později.

4. Činnost Správce při porušení zabezpečení osobních údajů

Pokud Správce zjistí, že došlo k porušení bezpečnosti osobních údajů, posoudí riziko pro subjekty údajů. Rizika jsou posuzována podle těchto kritérií:

- Typ porušení (zpřístupnění způsobí větší riziko než jejich úplná ztráta).
- Povaha, citlivost a objem osobních údajů (čím citlivější data, tím větší riziko pro jednotlivce, kombinace osobních údajů je více citlivá než samotná datová položka).
- Snadnost identifikace jednotlivců – někdy lze provést přímo z narušených osobních dat. Šifrovaná data bez šifrovacího klíče jsou pro nevolanou osobu nečitelná.
- Závažnost důsledků pro jednotlivce – u citlivých dat může být potenciální škoda pro jednotlivce zvlášť závažná, porušení osobních údajů u zranitelných jednotlivců může představovat vyšší riziko újmy. Dlouhodobé účinky mají větší dopad.
- Zvláštní charakteristiky jednotlivce – např. děti, lidé s postižením nebo zranitelné osoby.
- Počet dotčených jednotlivců – čím větší počet dotčených jednotlivců, tím větší dopad může porušení mít.
- Zvláštní charakteristiky správce – jsou rozdíly v citlivosti zpracovávaných osobních údajů.

Vyhodnocením rizik Správce může dospět k těmto závěrům:

a) Je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.
b) Je pravděpodobné, že porušení bude mít za následek riziko pro práva a svobody jednotlivců.
c) Je pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody jednotlivců. Vyšší riziko vznikne při porušení ochrany zvláštní kategorie osobních údajů (citlivých údajů).

Z vyhodnocení rizik podle a) nevyplývá Správci žádná ohlašovací resp. oznamovací povinnost.

Z vyhodnocení rizik podle b) vyplyne pro Správce ohlašovací povinnost k dozorovému úřadu.

Z vyhodnocení podle c) vyplyne pro Správce oznamovací povinnost k dozorovému úřadu a k subjektu údajů.

5. Ohlašovací povinnost Správce dozorovému úřadu

Ohlašovací povinnost dozorovému úřadu je spuštěna, jen když je pravděpodobné, že porušení bude mít za následek riziko pro práva a svobody jednotlivců.

Účelem ohlašovací povinnosti je omezení újmy způsobené fyzickým osobám. Porušení ochrany osobních údajů musí být nahlášeno nejpozději do 72 hodin dozorovému úřadu na některou z uvedených možností:

Adresa	**Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7**
E-mail	**posta@uoou.cz**
ID datové schránky	**qkbaa2n**

Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Pokud se porušení týkají stejného typu osobních údajů, jejichž zabezpečení bylo porušeno stejným způsobem během poměrně krátké doby, je možno provést hromadné ohlášení.

V ohlášení budou dozorovému úřadu poskytnuty alespoň tyto informace:[3]

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů (např. děti, lidé s postižením, zaměstnanci, zranitelné skupiny lidí atd.) a kategorií a přibližného množství dotčených záznamů osobních údajů (např. zdravotní data, školní záznamy, informace o sociální péči, finanční údaje, čísla bankovních účtů, čísla pasů atd.);
b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
d) 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.

6. Oznamovací povinnost Správce subjektu údajů

Oznamovací povinnost vůči jednotlivci je spuštěna, jen když je pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody jednotlivců, tj. porušení může vést u dotčeného jednotlivce k materiální nebo nemateriální škodě (diskriminaci, krádeži totožnosti, podvodu, peněžní ztrátě, poškození pověsti atd.).

Správce oznámí toto porušení bez zbytečného odkladu subjektu osobních údajů a dozorovému úřadu dle odstavce 5.

V oznámení subjektu údajů budou poskytnuty alespoň tyto informace:[4]

a) popis povahy porušení;
b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiné kontaktní místo;
c) popis pravděpodobných důsledků porušení;
d) popis opatření přijatých nebo navržených Správcem pro řešení případu, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Správce může poskytnout podle možností jednotlivcům konkrétní radu, jak se chránit před možnými nepříznivými důsledky porušení (např. resetování hesla apod.).

Oznámení subjektu údajů uvedené výše se nevyžaduje, je-li splněna kterákoli z těchto podmínek:[5]

a) Správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů. Jde zejména o taková opatření, která učinila tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování.
b) Správce přijal následná opatření, která zajistila, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví.
c) Vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Pokud dozorový úřad usoudí, že dané porušení bude mít s vysokou pravděpodobností za následek vysoké riziko, může na Správci požadovat, aby dotčenému subjektu údajů toto porušení oznámil, jestliže

[3] Obecné nařízení, článek 33, odstavec 3, písmeno a), b), c), d)
[4] Obecné nařízení, článek 33, odstavec 3, písmeno a), b), c), d)
[5] Obecné nařízení, článek 34, odstavec 3

tak dosud neučinil. Může však také rozhodnout, že je splněna některá z podmínek uvedených v předchozím odstavci.[6]

7. Odpovědnost a vedení záznamů

Dokumentace případů porušení – Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.[7] Správce vede dokumentaci o veškerých případech, i když nevznikne povinnost hlásit je dozorovému úřadu. Popis porušení musí obsahovat:

- popis události,
- příčiny porušení,
- jaké osobní údaje byly dotčeny,
- účinky a důsledky porušení,
- nápravná opatření přijatá správcem,
- zdůvodnění případného neohlášení incidentu resp. porušení důvody odkladu při opožděném podání ohlášení,
- doklad o oznámení subjektům osobních údajů,
- doklad o tom, že zaměstnanci Správce byli poučeni o tom, jak se mají v případě porušení zabezpečení osobních údajů zachovat.

Obdobným způsobem Správce zaznamená bezpečnostní incidenty, u nichž se okamžitě neprojevilo porušení zabezpečení osobních údajů, ale zároveň není vyloučeno, že se toto porušení neprojeví později.

Role pověřence pro ochranu osobních údajů – pověřenec spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro dozorový úřad a subjekty údajů. Jméno a kontakt na pověřence uvádí Správce při ohlašování události.

8. Poučení zaměstnanců

Správce seznámil své zaměstnance s obsahem této směrnice a poučil je o tom, jak se mají chovat, aby předcházeli případům porušení zabezpečení osobních údajů, a jak se chovat v případech, kdy k tomuto porušení dojde.

Poučení zaměstnanců se provádí při nástupu do zaměstnání, dále pravidelně jednou za 2 roky.

Jakýkoliv bezpečnostní incident zaměstnanci nahlásí svému vedoucímu zaměstnanci, který kontaktuje odpovědné osoby správce (viz. čl. 3.) nebo na telefonním čísle 389 822 802. V případě, že došlo k porušení zabezpečení osobních údajů, kontaktují pověřence pro ochranu osobních údajů.

9. Zpracovatel a jeho povinnosti

Pokud Správce používá Zpracovatele a tento Zpracovatel zjistí porušení zabezpečení osobních údajů, jež pro Správce zpracovává, musí to Správci ohlásit bez zbytečného odkladu.

Poskytuje-li Zpracovatel služby více Správcům, kteří všichni byli postiženi tím samým incidentem, musí Zpracovatel ohlásit podrobnosti o tomto incidentu všem Správcům.

---

[6] Obecné nařízení, článek 34, odstavec 4
[7] Obecné nařízení, článek 33, odstavec 5

Pokud osobní údaje byly učiněny nesrozumitelnými pro neoprávněné strany a jsou kopií nebo existuje záloha, pak porušení důvěrnosti řádně zašifrovaných osobních údajů nemusí být ohlášeno dozorovému úřadu.

Přílohy:

- č. 1: Postup při bezpečnostním incidentu a porušení zabezpečení ochrany osobních údajů a ohlašování události dozorovému úřadu a dotčeným osobám – slovní popis.
- č. 2: Postup při bezpečnostním incidentu a porušení zabezpečení ochrany osobních údajů a ohlašování události dozorovému úřadu a dotčeným osobám – schéma.
- č. 3: Formulář pro ohlašování porušení bezpečnosti osobních údajů dozorovému úřadu.
- Č. 4: Záznam bezpečnostního incidentu při ochraně osobních údajů.
- č. 5: Formulář pro oznámení porušení bezpečnosti osobních údajů subjektu osobních údajů.
- č. 6: Příklady bezpečnostních incidentů a porušení ochrany bezpečnosti osobních údajů.

Tento vnitřní předpis nabývá účinnosti dne: 7.5.2019.

V Soběslavi Dne: 7.5.2019

Střední škola řemeslná a Základní škola,
Soběslav, Wilsonova 405
IČ: 72549572

Ing. Darja Bártová

ředitelka SŠŘ a ZŠ Soběslav

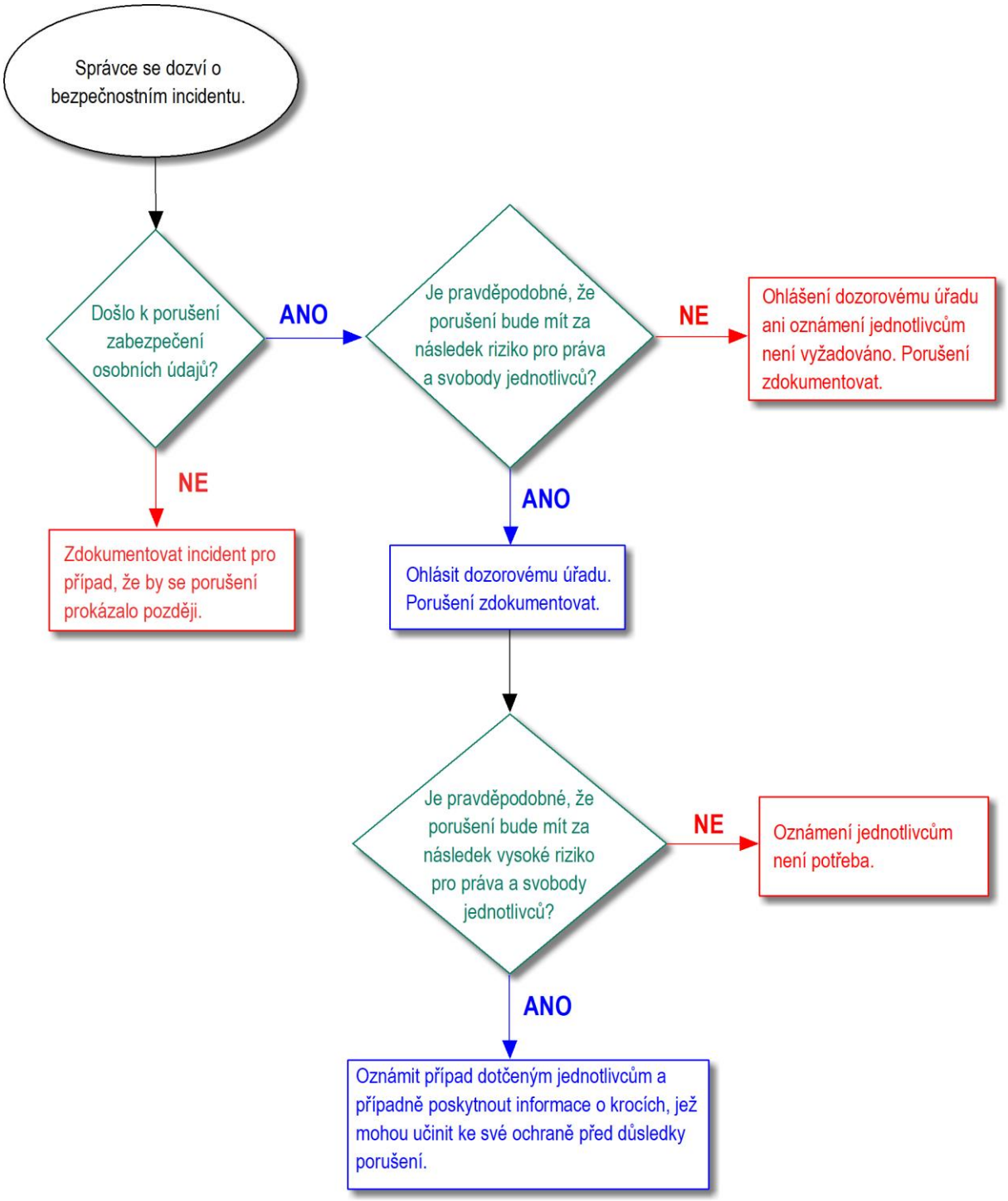
Příloha č. 1:

Postup při bezpečnostním incidentu a porušení zabezpečení ochrany osobních údajů a ohlašování události dozorovému úřadu a dotčeným osobám

1. Správce nebo jeho zaměstnanci se dozví o bezpečnostním incidentu. Neprodleně kontaktují odpovědnou osobu. Ta zjistí, zda došlo k porušení zabezpečení osobních údajů a posoudí riziko pro jednotlivce.
2. Došlo k porušení zabezpečení osobních údajů?
    a. NE. Zdokumentovat incident pro případ, že by se porušení prokázalo později. Použít formulář v Příloze č. 3.
    b. ANO – viz bod 3.
3. Je pravděpodobné, že porušení bude mít za následek riziko pro práva a svobody jednotlivců?
        i. NE. Ohlášení dozorovému úřadu ani oznámení jednotlivcům není potřeba.
        ii. ANO – viz bod 4.
4. Ohlásit porušení dozorovému úřadu s použitím formuláře v Příloze č. 3.
    a. Je pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody jednotlivců?
        i. NE. Oznámení jednotlivcům není potřeba.
        ii. ANO – viz bod 5.
5. Oznámit případ dotčeným jednotlivcům na formuláři v Příloze č. 4 a případně poskytnout informace o krocích, jež mohou učinit ke své ochraně před důsledky porušení.

Příloha č. 2:

Postup při bezpečnostním incidentu a porušení zabezpečení ochrany osobních údajů a ohlašování události dozorovému úřadu a dotčeným osobám.



Příloha č. 3: Formulář pro ohlašování porušení zabezpečení osobních údajů dozorovému úřadu

HLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ DOZOROVÉMU ÚŘADU

Správce osobních údajů	Klepněte sem a zadejte název organizace.
Pověřenec pro ochranu osobních údajů	Zařízení pro další vzdělávání pedagogických pracovníků a Středisko služeb školám, České Budějovice, Nemanická 7, Ing. Miroslava Nejezchlebová, e-mail: gdpr@zvas.cz; telefon: 608 057 836
Jméno a příjmení ohlašovatele	Klepněte sem a zadejte jméno a příjmení toho, kdo ohlašuje porušení.
E-mail ohlašovatele	Klepněte sem a zadejte e-mail toho, kdo ohlašuje porušení.
Telefon ohlašovatele	Klepněte sem a zadejte telefonní číslo toho, kdo ohlašuje porušení.
Datum bezpečnostního incidentu – porušení ochrany zabezpečení osobních údajů	Klepněte sem a zadejte datum.
Čas zjištění	Klepněte sem a zadejte čas ve formátu HH.MM.
Datum ohlášení dozor. úřadu	Klepněte sem a zadejte datum.
Čas ohlášení dozorovému úřadu	Klepněte sem a zadejte čas ve formátu HH.MM.
Datum oznámení subjektu OÚ	Klepněte sem a zadejte datum ve formátu DD.MM.RRRR.
Čas oznámení subjektům OÚ	Klepněte sem a zadejte čas ve formátu HH.MM.
Příčina porušení	
Viník porušení	
Popis události	
Dotčené osobní údaje	
Kategorie dotčených subjektů údajů	zaměstnanci ☐, děti ☐, žáci ☐, studenti ☐
Odhad počtu dotčených subjektů údajů	
Míra rizika	Zvolte položku.
Způsob porušení	Zvolte položku.
Typ porušení	Zvolte položku.
Účinky a důsledky	Zvolte položku.
Přijatá nápravná opatření	
Důvod neohlášení	Zvolte položku.
Důvod opožděného ohlášení	
Doklad o oznámení subjektům osobních údajů	Zvolte položku. ze dne Klepněte sem a zadejte datum., č. j. Klepněte sem a zadejte číslo jednací.
Doklad o poučení zaměstnanců pro případ porušení zabezpečení osobních údajů.	Přiložena kopie zápisu z porady konané dne Klepněte sem a zadejte datum. a prezenční listina přítomných zaměstnanců.

V Klepněte sem a zadejte místo. Dne: Klepněte sem a zadejte datum.

_____

jméno a podpis ohlašovatele

Příloha č. 4: Záznam bezpečnostního incidentu při ochraně osobních údajů

ZÁZNAM BEZPEČNOSTNÍHO INCIDENTU PŘI OCHRANĚ OSOBNÍCH ÚDAJŮ (interní materiál)

Správce osobních údajů	Klepněte sem a zadejte název organizace.
Pověřenec pro ochranu osobních údajů	Zařízení pro další vzdělávání pedagogických pracovníků a Středisko služeb školám, České Budějovice, Nemanická 7, Ing. Miroslava Nejezchlebová, e-mail: gdpr@zvas.cz; telefon: 608 057 836
Jméno a příjmení ohlašovatele	Klepněte sem a zadejte jméno a příjmení toho, kdo ohlašuje porušení.
E-mail ohlašovatele	Klepněte sem a zadejte e-mail toho, kdo ohlašuje porušení.
Telefon ohlašovatele	Klepněte sem a zadejte telefonní číslo toho, kdo ohlašuje porušení.
Datum bezpečnostního incidentu	Klepněte sem a zadejte datum.
Čas zjištění bezp. incidentu	Klepněte sem a zadejte čas ve formátu HH.MM.
Příčina porušení	
Viník porušení	
Popis události	
Dotčené osobní údaje	
Kategorie dotčených subjektů údajů	zaměstnanci ☐, děti ☐, žáci ☐, studenti ☐
Odhad počtu dotčených subjektů údajů	
Míra rizika	Zvolte položku.
Způsob porušení	Zvolte položku.
Typ porušení	Zvolte položku.
Účinky a důsledky	Zvolte položku.
Přijatá nápravná opatření	
Důvod neohlášení pověřenci pro OOÚ	Zvolte položku.
Důvod opožděného ohlášení pověřenci pro OOÚ	
Datum poučení zaměstnanců pro případ bezpečnostních incidentů	Klepněte sem a zadejte datum.

V Klepněte sem a zadejte místo. Dne: Klepněte sem a zadejte datum.

_____

jméno a podpis ohlašovatele

Příloha č. 5: Formulář pro oznamování porušení zabezpečení osobních údajů subjektu údajů

Titul subjektu údajů
Jméno a příjmení subjektu údajů
Adresa subjektu údajů
PSČ a místo bydliště subjektu údajů

Váš dopis / značka ze dne Naše značka Vyřizuje / linka Místo Datum

Oznámení o porušení zabezpečení osobních údajů

Zvolte položku,

v rámci naší povinnosti Vás informujeme o incidentu bezpečnosti dat, který Zvolte položku ohrožení Vašich osobních údajů, které zpracováváme.

Dne Klepněte sem a zadejte datum došlo k bezpečnostnímu incidentu: Klepněte sem a zadejte popis bezpečnostního incidentu.

Ohrožená data Zvolte položku tyto osobní údaje: Klepněte sem a zadejte typy ohrožených osobních údajů.

Podrobnou analýzou bylo vyloučeno, že by byly ohroženy následující osobní údaje: Klepněte sem a zadejte typ neohrožených osobních údajů.

S ohledem na výše uvedení zjištění si Vás dovolujeme upozornit, že následkem incidentu by mohlo dojít k Klepněte sem a zadejte možné následky. Proto doporučujeme Klepněte sem a zadejte stručné doporučení pro minimalizaci následků bezpečnostního incidentu.

Velice si vážíme Vašich osobních údajů a Vaší důvěry. Jako správce osobních údajů bereme vážně veškeré bezpečnostní incidenty a neprodleně po zjištění výše specifikovaného narušení zabezpečení jsme přijali následná opatření: Klepněte sem a zadejte popis přijatých opatření.

Dovolujeme si Vás ujistit, že naše (společnost/úřad) podnikl/a veškeré nutné kroky k minimalizaci rizika a v současné době plně pracuje s dozorovým orgánem na plném objasnění všech skutečností a na co nejrychlejší nápravě.

Pro další podrobnosti můžete kontaktovat našeho pověřence ochrany osobních údajů, a to e-mailem na gdpr@zvas.cz nebo na telefonu 608 057 836.

S pozdravem

_____

jméno a podpis osoby zastupující správce

Příloha č. 6:

Příklady bezpečnostních incidentů a porušení ochrany bezpečnosti osobních údajů

PŘÍKLAD č. 1	
Popis incidentu	Správce uložil záložní kopii archivu osobních údajů v zašifrované podobě na CD (DVD). Toto CD (DVD) bylo odcizeno během vloupání.
Ohlásit dozorovému úřadu?	Ne.
Ohlásit subjektu údajů?	Ne.
Poznámka	Data musí být zašifrovaná a zálohovaná, jedinečný klíč nebyl prozrazen. Dojde-li k jeho pozdějšímu prolomení, je ohlášení nutné.

PŘÍKLAD č. 2	
Popis incidentu	Ztráta CD nebo DVD s nezašifrovanými daty.
Ohlásit dozorovému úřadu?	Ano.
Ohlásit subjektu údajů?	Ano, pokud je subjekt údajů ohrožen vysokým rizikem.
Poznámka	Není možné ověřit, zda k osobním údajům získala neoprávněná osoba.

PŘÍKLAD č. 3	
Popis incidentu	Ztráta bezpečně zašifrovaného mobilního zařízení využívaného správcem a jeho zaměstnanci.
Ohlásit dozorovému úřadu?	Ne.
Ohlásit subjektu údajů?	Ne.
Poznámka	Při prozrazení šifrovacího klíče nebo při zjištění, že šifrovací software nebo algoritmus je zranitelný, stoupá úroveň rizika.

PŘÍKLAD č. 4	
Popis incidentu	Ztráta nezašifrovaného mobilního zařízení využívaného správcem a jeho zaměstnanci.
Ohlásit dozorovému úřadu?	Ano.
Ohlásit subjektu údajů?	Ano, pokud je subjekt údajů ohrožen vysokým rizikem.
Poznámka	

PŘÍKLAD č. 5	
Popis incidentu	Během kybernetického útoku byly z webové stránky provozované správcem získány osobní údaje jednotlivců.
Ohlásit dozorovému úřadu?	Ano – pokud hrozí možné důsledky pro jednotlivce.
Ohlásit subjektu údajů?	Ano – podle povahy dotčených osobních údajů v případě vysoké závažnosti případných dopadů na jednotlivce.
Poznámka	

PŘÍKLAD č. 6	
Popis incidentu	Správce utrpí útok ransomwarem (vyděračským softwarem), při němž dojde k zašifrování dat. Jiný škodlivý software (mallware) nebyl zjištěn. K dispozici jsou zálohy a data lze obnovit.
Ohlásit dozorovému úřadu?	Ne.

Ohlásit subjektu údajů?	Ne.
Poznámka	Nejedná se o trvalou ztrátu dostupnosti osobních údajů.

PŘÍKLAD č. 7	
Popis incidentu	Správce utrpí útok ransomwarem (vyděračským softwarem), při němž dojde k zašifrování dat. Jiný škodlivý software (mallware) nebyl zjištěn. Zálohy nejsou k dispozici a data nelze obnovit.
Ohlásit dozorovému úřadu?	Ano.
Ohlásit subjektu údajů?	Ano.
Poznámka	Jde o případ trvalé ztráty dostupnosti nebo důvěrnosti.

PŘÍKLAD č. 8	
Popis incidentu	Osobní údaje žáků (studentů) byly omylem poslány na nesprávný adresář obsahující adresy různých příjemců.
Ohlásit dozorovému úřadu?	Ano.
Ohlásit subjektu údajů?	Ano – oznámení bude záviset na typech a množství dotčených osobních údajů spojených s vysokým rizikem pro subjekty osobních údajů.
Poznámka	

PŘÍKLAD č. 9	
Popis incidentu	E-mail v rámci přímého marketingu byl odeslán příjemcům v kolonce *Komu* nebo *Kopie*, čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.
Ohlásit dozorovému úřadu?	Ano v případě postižení většího počtu jednotlivců, došlo k odhalení citlivých údajů nebo existují jiné faktory představující vysoké riziko.
Ohlásit subjektu údajů?	Ano – oznámení bude záviset na typech a množství dotčených osobních údajů spojených s vysokým rizikem pro subjekty osobních údajů.
Poznámka	Ohlášení nemusí být nutné, pokud nedošlo k odhalení citlivých údajů nebo došlo k odkrytí jen malého počtu e-mailových adres.