

Ochrana osobních údajů

Výroční zpráva

za rok 2024

(interní dokument pro potřeby správce)

SBOU . CZ

Správce: Základní škola Dubá
Dlouhá 113
471 41 Dubá
IČ: 48282979

Vypracoval: Ing. Milan Ištok (istok@sbou.cz)
Stvolínky 38
471 02 Stvolínky
tel. 608 000 392

Datum zpracování: 8.12.2024

Verze: 1.0

Změny:

0.5	30.10.2024	Pracovní, přípravná verze
0.8	7.11.2024	Doplněná verze
1.0	8.12.2024	Revidovaná a odsouhlasená verze

Správce osobních údajů

Správce: Základní škola Dubá
Dlouhá 113
471 41 Dubá
IČ: 48282979

Kontaktní osoba: ředitel Mgr. Jana Heringová

Pověřenec na ochranu osobních údajů:

Ing. Milan Ištok (istok@sbou.cz)
Stvolínky 38
471 02 Stvolínky
tel. 608 000 392

Úvod

Správce jmenoval do **pozice pověřence Ing. Milana Ištoka** na základě čl. 37 odst. 1 písm. a) 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 a o zrušení směrnice 95/46/ES (dále jen „nařízení o ochraně osobních údajů“ či „GDPR“).

Ing. Milan Ištok je členem Spolku pro ochranu osobních údajů, které sdružuje pověřence pro ochranu osobních údajů a další odborníky zabývající se zpracováním a ochranou osobních údajů v soukromém sektoru, samosprávě a státní správě. Kromě toho se účastní školení pořádaných spolkem nebo pod patronací spolku. Kromě toho se účastní také přednášek pořádaných Národním úřadem pro kybernetickou bezpečnost (dále též „NUKIB“), které se týkají kybernetické bezpečnosti.

Konkrétně se v roce 2024 účastnil těchto přednášek a školení:

- Nařízení Evropského parlamentu a Rady (EU) 2023/2854) - Data Act
- Nařízení Evropského parlamentu a Rady (EU) 2024/1689 - AI Data
- Kamery ve školách z pohledu GDPR
- Realizace práva na informace v kontextu ochrany osobních údajů a soukromí (Zákon č. 106/1999 Sb., o svobodném přístupu k informacím)
- Praktické aspekty kontroly cookies

Pověřenec na ochranu osobních údajů byl jmenován a nahlášen na Úřad na ochranu osobních údajů.

Kontaktní údaje pověřence osobních údajů jsou zveřejněny na webových stránkách správce, a to v rozsahu jméno, příjmení, email a telefonní kontakt.

Pověřenec na ochranu osobních údajů byl jmenován a nahlášen na Úřad na ochranu osobních údajů.

Úkoly vyplývající z ochrany osobních údajů

Pověřenec pro ochranu osobních údajů v rámci organizace je pověřen především úkoly vyplývajícími z čl. 39 odst. 1, čl. 38 odst. 4 nebo čl. 30 nařízení o ochraně osobních údajů.

- poskytování informací a poradenství správcům a zaměstnancům, kteří provádějí zpracování osobních údajů, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
- monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů,
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35,
- spolupracuje s dozorovým úřadem,
- působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vede konzultaci v jakékoli jiné věci,
- působí jako kontaktní osoba, na kterou se mohou obracet subjekty ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle nařízení, přesto je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, a to v souladu s právem Unie nebo členského státu
- ve spolupráci se správcem vede záznamy o činnostech zpracování
- provádí posuzování rizikovosti zpracování osobních údajů a souladu tohoto zpracování v organizaci
- pověřenec se podle požadavků správce spolupodílí na vypracování a udržování zásad pro zpracování osobních údajů v rámci organizace
- v případě zásadních změn zpracování osobních údajů nebo v případě zavádění nových způsobů zpracování osobních údajů, se podílí na posuzování rizikovosti zpracování osobních údajů
- zajišťuje školení zaměstnanců určených správcem v oblasti ochrany osobních údajů a oblasti kybernetické bezpečnosti
- pověřenec spolupracuje se správcem v případě řešení případů týkajících se porušení zabezpečení osobních údajů
- pověřenec informuje správce o současné situaci v oblasti zpracovávání osobních údajů či o případných požadavcích v této oblasti
- v případě že by některý druh zpracování mohl vést k vyššímu riziku pro ochranu osobních údajů, provádí pověřenec posouzení tohoto zpracování a případně balanční test

Přijatá opatření k zajištění souladu s právními předpisy týkajícími se ochrany osobních údajů správcem osobních údajů

V souvislosti s nařízením o ochraně osobních údajů a dalšími souvisejícími právními normami (tzv. implementační zákon č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů) přijal správce od jmenování pověřence následující opatření, která mají zajistit soulad s pravidly ochrany osobních údajů:

- Správce provedl jmenování pověřence na ochranu osobních údajů podle čl. 37 GDPR.
- Správce přijal Směrnici o ochraně osobních údajů.
- Správce přijal Směrnici výpočetní techniky.
- Správce zveřejnil Informace o zpracování osobních údajů na webových stránkách.

- Správce aktualizoval Spisový řád a skartační plán
- Správce vede Záznamy o zpracování osobních údajů v souladu s čl. 30 GDPR.
- Správce provedl kontrolu a případné doplnění smluv (dodavatel SW, zpracovatelské smlouvy atd.).
- Zaměstnanci správce byli seznámeni s povinnostmi a právy vyplývajícími z ochrany osobních údajů (viz. Informace o ochraně osobních údajů pro zaměstnance).
- Správce připravil scénář plnění práv subjektů podle čl. 15 až 22 GDPR.
- Správce připravil scénář pro případ narušení ochrany osobních údajů.
- Správce je připraven vést v případě potřeby Evidenci souhlasů subjektů.
- Správce vede evidenci vydaných klíčů, kódů k EZS a vlastní kvalifikovaný elektronický podpis.
- Správci byla prověřena minimální bezpečnost výpočetní techniky (např. omezený fyzický přístup k počítačům, nastavená hesla, nainstalovaný antivirový program, aktualizovaný operační systém atd.)
- Správce provedl zajištění listinných dokumentů, a průběžně provádí skartaci listinných dokumentů podle aktuálního skartačního řádu.
- Určené osoby byly proškoleny v oblasti ochrany osobních údajů.
- Správce provádí anonymizaci zveřejňovaných dokumentů v souladu s principy nebo pravidly GDPR.
- Dochází k pravidelné kontrole dodržování ochrany osobních údajů (zejména uložení dokumentů s osobními údaji, kontrola aktuálnosti směrnic, aktualizace informací na webových stránkách, provádění záznamů o zpracování, zálohování dat, ...).

Pověřenec současně pravidelně a průběžně informuje správce o novinkách, které pomáhají zajistit a zlepšovat ochranu osobních údajů:

- Přijetí nařízení o ochraně osobních údajů a implementačního zákona č. 110/2019 Sb., o ochraně osobních údajů.
- Zákonné změny týkající se vedení spisové služby (informace z archivu Česká Lípa, změny vyplývající ze zákona č. 110/2019 Sb., o ochraně osobních údajů).
- Zákony týkající se elektronizace veřejné správy.
- Informace ze zpráv zveřejňovaných Úřadu pro ochranu osobních údajů, týkajících se ochrany osobních údajů.
- Informace vyplývající ze zpráv zveřejněných na stránkách Úřadu pro ochranu osobních údajů (např. Protokolů o kontrole).
- Potřeba zajistit přístupnost internetových stránek školy v souladu se zákonem.
- Informace o změnách právních předpisů, která se dotýkají zpracování osobních údajů.
- Zpřesnění posuzování kamerového systému ze strany Úřadu pro ochranu osobních údajů

Popis stávajícího stavu

Zpracování osobních údajů provádí správce obvyklým způsobem a v přiměřeném rozsahu. Listinné dokumenty jsou uchovávány v uzamykatelných prostorách nebo uzamykatelných skříních. Správce současně zajišťuje průběžnou archivaci a skartaci listinných dokumentů, kterým uplynula skartační lhůta.

Osobní údaje zpracováváné s pomocí elektronických zařízení jsou zpracováváné s pomocí výpočetní techniky, na které je pravidelně aktualizovaný operační systém, antivirový program a klíčová data jsou zálohována. Přístup k počítačům je fyzicky omezen (počítače jsou v uzamykatelných prostorech) a přístup umožněn jen s pomocí přístupového jména a hesla (autentizace a autorizace). Obsluha je

proškolená z hlediska kybernetické bezpečnosti – především phishing a zásady zacházení s osobními údaji.

Škola je umístěna ve zděné dvoupodlažní budově, ředitelna je umístěna v prvním patře.

Budova je uzamykatelná, a je zabezpečena elektronickým zabezpečovacím zařízením. Kromě toho jsou prostory školy zabezpečeny kamerovým systémem.

Pro zajištění bezpečnosti žáků a zaměstnanců školy, škola instalovala kamerový systém, který monitoruje vnitřní prostory školy.

Plnění práv subjektů údajů podle čl. 15 až 22 nařízení o ochraně osobních údajů

Pro plnění práv subjektů údajů podle čl. 15 až 22 nařízení o ochraně osobních údajů je připraven scénář, jak postupovat v případě, že subjekt údajů vznesl požadavek týkající se jeho práv. Tento scénář obsahuje konkrétní postupy, jak postupovat v případě žádostí subjektů.

V roce 2024 nebyl zaznamenán žádný požadavek subjektů údajů podle nařízení o ochraně osobních údajů.

Porušení zabezpečení osobních údajů

Správce byl informován o povinnostech vyplývajících z porušení zabezpečení osobních údajů ve smyslu čl. 33 nařízení o ochraně osobních údajů. Pro tento případ byl připraven scénář, jak postupovat v případě, že dojde k takovému porušení zabezpečení ochrany osobních údajů u správce (nebo jeho zpracovatelů).

V roce 2024 nebyl zaznamenán žádný případ porušení zabezpečení, který by ohrožoval osobní údaje subjektů.

Souhrn za rok 2024

V tomto roce byly provedeny kontroly a revize důležitých dokumentů pro ochranu osobních údajů.

Pověření zaměstnanci správce byli průběžně informováni o aktuálních novinkách v oblasti ochrany osobních údajů a kybernetické bezpečnosti.

Dále byl zástupce správce proškolen o zajištění bezpečnosti z hlediska kybernetické bezpečnosti, konkrétně o nutnosti zálohovat data, potřebnost používat silná hesla, nebezpečí phishingu a další.

V roce 2024 upřesnil Úřad na ochranu osobních údajů metodiku na hodnocení kamerových systémů. V souvislosti s tím došlo k rozšíření okruhu kamerových systémů, které jsou posuzovány z hlediska ochrany osobních údajů. Bylo tak nutné přepracovat posouzení kamerového systému.

V tomto roce dále probíhají přípravy na přechod na plně elektronickou spisovou službu. Jedná se především o zahájení certifikací spisových služeb, aktualizace spisového plánu a řádu, ale došlo k prodloužení lhůty k implementaci ESSL o rok.

V průběhu roku byla prováděna kontrola a revize záznamů o zpracování osobních údajů správce, kde docházelo k upřesnění a k aktualizaci některých údajů.

Kromě toho byly řešeny konkrétní dotazy správce týkající se zabezpečení a ochrany osobních údajů.

Pověřenec předal správci tyto dokumenty:

- Doklady o provedeném školení týkající se ochrany osobních údajů
- Záznamy o činnostech zpracování
- Posouzení rizik vyplývajících ze zpracování osobních údajů na základě záznamů o činnostech zpracování

Úkoly pro rok 2025

V příštím roce bude probíhat především monitorování souladu činnosti správce s nařízením o ochraně osobních údajů, s dalšími předpisy Evropské Unie, zákonem č. 110/2019 Sb., o ochraně osobních údajů a normami České republiky v oblasti ochrany osobních údajů, společně s koncepcemi správce nebo zpracovatele. Dále bude probíhat opakovaná kontrola a aktualizace dokumentů týkajících se ochrany osobních údajů, současně s kontrolou směrnic a záznamů o zpracování.

Konkrétně se u správce bude jednat o tyto úkoly:

- Revize směrnice Používání výpočetní techniky.
- Revize směrnice Ochrana osobních údajů.
- Revize rizik.
- Revize složky GDPR.
- Revize smluv se zpracovateli, pokud správce zpracovává osobní údaje pomocí správce.
- Revize informačního memoranda zveřejněných na internetových stránkách.
- Revize záznamů o činnosti zpracování.

Z hlediska bezpečnosti výpočetní techniky bude probíhat především kontrola funkčnosti záloh a obnovy a revize přístupových účtů a hesel, popřípadě rušení přístupových účtů bývalých zaměstnanců.

Co se týká webu, bude probíhat náhodná kontrola dokumentů uložených na webu správce, a to z hlediska zákonnosti umístění dokumentů na web, jejich aktuálnosti a případně správné anonymizace osobních údajů.

V průběhu roku, bude průběžně prováděna kontrola organizačních opatření:

- Kontrola kanceláře a archivu.
- Omezení množství dokumentů volně přístupných (např. na stolech, v odemčených skříních a na dalších nevhodných, nezabezpečených místech).
- Příprava na zavedení elektronického systému spisové služby.
- Provedení a nastavení pravidel odstranění nestrukturovaných dat z počítačů a archivu, které jsou součástí procesu elektronické skartace.
- Kontrola, že nejsou zpracovávány ani uchovávány žádné dokumenty elektronicky či fyzicky obsahující osobní údaje, na které neexistuje oprávnění pro zpracování nebo tomuto oprávnění již uplynula lhůta.

Kromě toho bude provedeno opakované školení pověřených osob správce z hlediska ochrany osobních údajů a kyberbezpečnosti.

Současně bude nutné reagovat na požadavky Úřadu pro ochranu osobních údajů, které se bude týkat upřesnění postupů, rozsahu dokumentů a činností dle informací Úřadu. Pověřenec se bude účastnit setkání pověřenců a získávat informace z odborných zdrojů nebo spolku pro zachování aktuálnosti jeho činnosti. K tomu se zavazuje předávat informace koordinátorovi GDPR.

V případě požadavku subjektů podle čl. 15 až 22 nařízení o ochraně osobních údajů nebo porušení zabezpečení osobních údajů, pověřenec zajistí řádné zpracování podle připraveného scénáře a poskytne potřebnou pomoc.

Bude provedeno posouzení zpracování osobních údajů v souvislosti s kamerovým systémem podle finální metodiky Úřadu na ochranu osobních údajů.

Je nutné zaměřit se na přípravu na přechod na elektronickou spisovou službu (uložení dokumentů a archivace).

Zhodnocení bezpečnosti osobních údajů zpracovávaných správcem

V průběhu roku docházelo k průběžnému posuzování zpracování osobních údajů správcem z hlediska nařízení o ochraně osobních údajů.

Zpracování osobních údajů probíhá v souladu s platnými právními předpisy týkajícími se ochrany osobních údajů, a to v obvyklém rozsahu nezbytném pro plnění úkolů a povinností.

Zpracování osobních údajů je prováděno v přiměřeném rozsahu, a to s ohledem na účel, pro který byly údaje shromážděny a v souladu s principy transparentnosti, spravedlnosti a zákonnosti.

Nebyly zjištěny problémy, které by se týkaly zpracování a ochrany osobních údajů.