Směrnice o ochraně osobních údajů a jejich nakládání s nimi

Směrnice o ochraně osobních údajů a jejich nakládání s nimi dle 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 (obecné nařízení o ochraně osobních údajů)

Název organizace: SOŠ dopravy a cestovního ruchu v Krnově, p. o.

Datum účinnosti: 25. 5. 2018

Verze: 1

I.
Obecná ustanovení

1) Tato směrnice o ochraně osobních údajů (dále také „směrnice") upravuje způsob nakládání s osobními údaji, které ***Střední odborné škole dopravy a cestovního ruchu v Krnově, p. o.*** (dále jen „organizace") zpracovává, tak aby byla zajištěna náležitá ochrana těmto osobním údajům dle platných právních předpisů, zejména dle 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 (obecné nařízení o ochraně osobních údajů) [dále jen „GDPR"].
2) Organizace zpracovává osobní údaje na základě některého z právních titulů, které vyjmenovává GDPR. Organizace nezpracovává osobní údaje bez právního titulu dle předchozí věty. Organizace zpracovává osobní údaje vždy za konkrétním účelem, který nesmí být v rozporu s platnými právními předpisy, zejména s GDPR.
3) Organizace při zpracovávání osobních údajů může vystupovat jako:
    a) správce osobních údajů, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za ně,
    b) zpracovatel osobních údajů, který zpracovává osobní údaje na základě zvláštního zákona nebo pověření správce.

II.
Vymezení odpovědnosti

1) Za zpracování osobních údajů, které organizace provádí, odpovídá vždy ředitel organizace. Ředitel organizace zodpovídá za to, že zpracování osobních údajů je prováděno v souladu s platnými právními předpisy, zejména v oblastech:
    a) plnění informační povinnosti k subjektům údajů,
    b) uplatňování práv subjektů údajů,
    c) zajištění technických a organizačních opatření na ochranu osobních údajů,
    d) spolupráce s pověřencem pro ochranu osobních údajů.
2) Ředitel organizace může pro oblast ochrany osobních údajů jmenovat odpovědnou osobu z řad pracovníků organizace, která bude také zodpovídat za ochranu osobních údajů, a to v rozsahu, který určí ředitel organizace (dále jen „odpovědná osoba"); odpovědnost ředitele organizace za zpracování osobních údajů dle této směrnice tím není nijak dotčena.
3) Odpovědnou osobou dle předchozího odstavce tohoto článku směrnice je: Mgr. Ladislav Mokráš, *zástupce ředitele.*
4) Organizace je povinna dle č. 37 a násl. jmenovat pověřence pro ochranu osobních údajů (dále jen „pověřenec"). Pověřenec vykonává svou funkci v souladu s příslušnými ustanoveními GDPR.
5) Moravskoslezský kraj jako zřizovatel organizace poskytuje metodickou pomoc v oblasti ochrany osobních údajů.

III.
Povinnosti organizace při zpracování osobních údajů

1) Organizace je při zpracování osobních údajů povinna:
    a) řádně stanovit právní titul, rozsah a účel zpracování osobních údajů,

b) průběžně monitorovat a případně upravit jednotlivá zpracování osobních údajů, v případě, že zpracování není v souladu s GDPR,

c) spolupracovat s pověřencem, s Moravskoslezským krajem jako zřizovatelem organizace a orgány veřejné moci při plnění jejich oprávnění v oblasti ochrany osobních údajů,

d) v případě využití zpracovatele osobních údajů uzavřít smlouvu o zpracování osobních údajů, která bude v souladu s čl. 28 GDPR; pokud nejsou při využití zpracovatele osobních údajů splněny jiné předpoklady ke zpracování dle GDPR,

e) u nového zpracování osobních údajů si vyžádat konzultaci pověřence, a to ještě před zahájením zpracování osobních údajů.

2) Ředitel organizace je povinen:

a) zajistit, aby zpracování osobních údajů prováděné organizací bylo v souladu se zásadami GDPR; zejména zásadou zákonnosti zpracování, minimalizace a přiměřenosti zpracování, korektnosti a transparentnosti zpracování,

b) zajistit plnění informační povinnost dle čl. 13 GDPR, zejména prostřednictvím webových stránek organizace a tiskopisů, které organizace používá (např. přihlášky, formuláře apod.),

c) zajistit vedení záznamů o zpracování osobních údajů,

d) zajistit oznamování bezpečnostních incidentů ve spolupráci s pověřencem, dozorovému úřadu dle čl. 33 a násl. GDPR,

e) zajistit náležitou ochranu osobních údajů, a to prostřednictvím přijetí opatření technického a organizačního charakteru,

f) zajistit výkon práv subjektů údajů dle čl. 15 a násl. GDPR, tj. práva na informace o zpracování, provedení výmazu, opravy či omezení zpracování osobních údajů,

g) vyžádat si stanovisko pověřence při provádění rizikových operací s osobními údaji, např. předávání do ciziny, použití automatizovaného zpracování osobních údajů či použití prostředků pro zpracování osobních údajů, které mohou výrazně zasahovat do soukromí subjektů údajů (např. čtečky otisků prstů, kamerové systémy, sledování polohy subjektů údajů prostřednictvím GPS).

3) Ředitel organizace je při zpracování osobních údajů povinen zajistit, aby:

a) osobní údaje byly zpracovávány v souladu s platnými právními předpisy i v případě, že jsou zpracovávány prostředky výpočetní techniky, v rámci informačních systémů, aplikací atp.,

b) všechny osoby, které se podílejí na zpracování osobních údajů, zachovávaly mlčenlivost o těchto osobních údajích,

c) osobní údaje obsažené ve spisech a dokumentech byly zpracovávány pouze osobami, které jsou k tomu pověřené ředitelem organizace; jiné osoby nesmí mít k osobním údajům přístup a nesmí je zpracovávat,

d) byly stanoveny pracovníkům organizace pravidla pro uchovávání dokumentů (a jiných nosičů) s osobními údaji v uzamykatelných prostorách,

e) osobní údaje, které nelze zpracovávat na základě jiného právního titulu, než je souhlas se zpracováním osobních údajů, byly zpracovávány pouze s tímto souhlasem,

f) vést evidenci souhlasů se zpracováním osobních údajů,

g) při předávání osobních údajů uvnitř organizace zajistit, aby byly předávány pouze osobám, které jsou ke zpracování osobních údajů pověřeny ve smyslu písm. c) tohoto odstavce,

h) k předávání osobních údajů mimo organizaci docházelo pouze, pokud tak stanoví právní předpis, platně uzavřená smlouva anebo je k takovému předávání udělen souhlas dotčeného subjektu údajů,

i) při komunikaci organizace s veřejností (případně při vedení správního či daňového řízení též s účastníky řízení), a to v jakékoliv formě (ústně, písemně, elektronicky), při které dochází ke zpracování osobních údajů, bylo postupováno v souladu s právními předpisy,

j) byly dokumenty v listinné podobě obsahující osobní údaje ukládány způsobem zamezujícím neoprávněnému či nahodilému přístupu neoprávněných osob k těmto dokumentům (uzamykatelné místnosti, skříně, šuplíky apod.),

k) nebyly pořizovány kopie dokumentů obsahujících osobní údaje pro jiné využití, než které souvisí s činností organizace,

l) v případě zjištění porušení zabezpečení osobních údajů (nebo nabytí podezření o takovém porušení) neprodleně, nejpozději do 24 hodin, od okamžiku, kdy se o něm dozvěděl informovat bezprostředně pověřence; bližší postup ohlášení a evidence porušení zabezpečení osobních údajů je uveden v příloze č. 2 této směrnice.

IV.
Organizační a technická opatření související s ochranou osobních údajů

1) Organizace je povinna přijmout technická a organizační opatření k zajištění náležité ochrany osobních údajů s ohledem ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům, rizikům pro práva svobody fyzických osob, k zamezení neoprávněného nebo nahodilého přístupu, změně, zničení či ztrátě, alespoň v rozsahu uvedeném v tomto článku.

2) Organizace je povinna přijmout a dodržovat tato organizační opatření:

   a) Osoby provádějící zpracování osobních údajů mají stanoveny povinnosti ke zpracování osobních údajů, zejména prostřednictvím právních předpisů, pracovních smluv a jiných vnitřních předpisů organizace.

   b) Dochází-li ke zveřejňování dokumentů, obsahujících osobní údaje je nutné provést anonymizaci osobních údajů, ledaže je jejich zveřejnění stanoveno zvláštním právním předpisem.

3) Organizace je povinna přijmout a dodržovat tato personálně-organizační opatření:

   a) Osoby provádějící v organizaci zpracování osobních údajů mají v rámci své pracovní náplně (či jiným obdobným opatřením) stanoven rozsah oprávnění k přístupu a zpracování osobních údajů zachycených ve fyzické podobě. Stejně tak je jim stanoven rozsah oprávnění přístupu do informačních systémů a aplikací, ve kterých jsou zpracovávány osobní údaje zachycené v elektronické podobě. O rozsahu takových přístupů je u každé osoby veden záznam.

   b) Pracovníci organizace jsou při zahájení pracovního poměru seznámeni s vnitřními předpisy organizace, zejména v oblasti ochrany osobních údajů. Pracovníci organizace jsou informováni o aktuálním stavu právních předpisů (zejména novelizacích příslušných právních předpisů) výkladové a rozhodovací praxi v oblasti ochrany osobních údajů.

4) Organizace je povinna přijmout a dodržovat tato administrativně-organizační bezpečnostní opatření:
    a) Dokumenty či spisy, které obsahují osobní údaje, mohou zpracovávat pouze osoby, které jsou k tomu oprávněny, a to na základě jejich pracovního zařazení či jiného oprávnění dle právního předpisu.
    b) Při provádění kontrol, nahlížení účastníků řízení do spisu při vedení správního či daňového řízení či jiné činnosti, při které by mohly osobní údaje zpřístupněny dalším osobám, je nutné zajistit ochranu těm osobním údajům, které nesouvisejí s prováděnou činností.
    c) Dokumenty obsahující osobní údaje nesmí být vynášeny mimo prostory organizace, pokud tak není činěno na základě právního předpisu; v ostatních případech je vynášení dokumentů obsahujících osobní údaje možné jen ve výjimečných případech a po přechozím souhlasu ředitele organizace.
    d) Dokumenty obsahující osobní údaje jsou ukládány tak, aby nedošlo ke zneužití osobních údajů, a to zejména uložením v uzamykatelných místnostech či skříních.
    e) Organizace při manipulaci s dokumenty postupuje dle platného spisového a skartačního řádu.
5) Organizace je povinna přijmout a dodržovat tato opatření v oblasti zabezpečení prostředků výpočetní techniky:
    a) Osobní údaje, které jsou zpracovávány v rámci počítačové sítě, informačních systémů, aplikací a zařízeních (zejména počítače, servery, tiskárny, kopírky, mobilní telefony, tablety), jsou chráněny tak, aby nedošlo k jejich zneužití. Výše uvedená zařízení jsou zabezpečena tak, aby k nim neměly přístup neoprávněné osoby.
    b) Přístup k počítačové síti a zařízením dle písm. a) je zabezpečen prostřednictvím autentizace a autorizace, tedy použitím přihlašovacího jména a hesla či jiným obdobným bezpečnostním prvkem.
    c) Významné součásti počítačové sítě, informačních systémů a aplikací provozovaných organizací (zejména servery a datová úložiště) jsou umístěny v prostorách, které jsou přístupné pouze osobám pověřeným ředitelem organizace.
    d) Zařízení dle písm. a) musí být chráněna antivirovým a antimalware softwarem, případně dalším bezpečnostním softwarem.
    e) Data uložená v počítačové síti a zařízeních jsou pravidelně a plánovaně zálohována a uchovávána.
    f) Aplikace a informační systémy, ve kterých jsou zpracovávány osobní údaje, vytvářejí auditní záznamy, ohledně přístupu k osobním údajům jednotlivými koncovými uživateli, tak aby bylo možné zjistit, jaká osoba měla k osobním údajům přístup. Auditní záznamy jsou zabezpečeny proti jejich modifikacím.
    g) Přístup externích osob do počítačové sítě, informačního systému či aplikace je umožněn pouze osobám, na základě schválení ředitele organizace či osoby pověřené ředitelem organizace.
6) Organizace je povinna přijmout a dodržovat tato kontrolní opatření:
    a) Ředitel organizace kontroluje oblast ochrany osobních údajů, a to zejména:
        - ukládání spisů a dokumentů obsahujících osobní údaje;
        - oprávněnost prováděných zpracování osobních údajů z pozice platného právního titulu a účelu zpracování;

- přístup k prostředkům výpočetní techniky a jejich dostatečnému zabezpečení,
- dodržování dalších povinností uložených právními předpisy v oblasti ochrany osobních údajů.

b) Organizace je povinna při realizaci kontrolních opatření dle písm. a) tohoto odstavce spolupracovat také s pověřencem a Moravskoslezským krajem jako zřizovatelem organizace.

V.
Závěrečná ustanovení

1) Tato směrnice nabývá účinnosti dne 25. 5. 2018.
2) Tato směrnice nahrazuje veškeré přechozí směrnice, vnitřní předpisy a jiné dokumenty související s ochranou osobních údajů, které byly vydány organizací.
3) Nedílnou součástí této směrnice jsou tyto přílohy:

   Příloha č. 1: Postup k vyřízení žádosti dle čl. 15 až 20 GDPR

   Příloha č. 2: Postup nahlášení bezpečnostního incidentu dle čl. 33 a násl. GDPR

V Krnově dne 24. 5. 2018

Mgr. Zdeněk Klein
ředitel organizace

Příloha č. 1

Postup k vyřízení žádosti dle čl. 15 až 20 GDPR

1) Tento postup je organizací využit v případě, kdy subjekt údajů, či jiná osoba vykonávající práva subjektu údajů (dále jen „žadatel"), uplatní prostřednictvím žádosti práva dle čl. 15 až 20 GDPR (dále jen „žádost") vůči organizaci.
2) Za vyřízení žádosti odpovídá ředitel organizace.
3) Žádost může žadatel podat prostřednictvím písemného podání zaslaného běžnou poštou, elektronickou poštou, datovou schránkou nebo ústně do protokolu.
4) Totožnost žadatele je ověřena v případě, že žádost je ve fyzické podobě opatřena jasnými identifikačními údaji žadatele a jeho podpisem. Totožnost je také ověřena, pokud je žádost v elektronické podobě opatřena zaručeným elektronickým podpisem a nepanují pochybnosti o totožnosti žadatele. Totožnost žadatele je rovněž ověřena v případě, kdy byla žádost podána ústně do protokolu, přičemž byla totožnost žadatele zjištěna z dokladu totožnosti či jiného dokladu. V případě, že je žádost podána elektronicky bez zaručeného elektronického podpisu a z okolností nevyplývá totožnost žadatele, je organizace povinna vyzvat žadatele k objasnění své totožnosti dle předchozí věty.
5) Pokud bude žadatel požadovat kopii osobních údajů ve smyslu čl. 15 odst. 3 GDPR, je žadatel povinen žádost podat s úředně ověřeným podpisem, elektronicky se zaručeným elektronickým podpisem, datovou schránkou nebo osobně do protokolu po ověření totožnosti dle předchozího odstavce. Bez takového ověření nelze vydat kopie osobních údajů. Kopie osobních údajů budou vydávány do vlastních rukou žadatele.
6) Jestliže žádost obdrží kterýkoliv pracovník organizace, je povinen ji okamžitě postoupit řediteli organizace.
7) Po obdržení žádosti vyrozumí ředitel o této skutečnosti pověřence a pověřence Moravskoslezského kraje, a to v následujícím rozsahu:
    - datum přijetí žádosti,
    - popis obsahu žádosti, tzn. které právo subjektu údajů dle je uplatňováno,
    - předpokládaný termín vyřízení žádosti.
8) Po vyřízení žádosti vyrozumí ředitel pověřence a pověřence Moravskoslezského kraje o datu a způsobu vyřízení žádosti.
9) V případě, kdy jsou podávány žádosti zjevně nedůvodné, nepřiměřeně či opakované, je organizace oprávněna žádost odmítnout. Odmítnutí musí být řádně odůvodněno.

Příloha č. 2

Postup nahlášení bezpečnostního incidentu dle čl. 33 GDPR

1) Tento postup je organizací využit v případě, kdy je nutné dozorovému úřadu (tj. Úřadu pro ochranu osobních údajů) porušení zabezpečení osobních údajů dle čl. 33 a násl. GDPR (dále jen „bezpečnostní incident").
2) Za oznámení bezpečnostního incidentu dozorovému úřadu odpovídá ředitel organizace.
3) Za bezpečnostní incident je považováno takové narušení zabezpečení osobních údajů, které by mohlo způsobit náhodné či protiprávní zničení, ztrátu, změnu, zpřístupnění či přenesení osobních údajů zpracovávaných organizací. Příkladem bezpečnostního incidentu může být např. odcizení dokumentů obsahujících osobní údaje, vážná porucha serveru atd.
4) Ihned po zjištění, nejpozději do 48 hodin, možného bezpečnostního incidentu ředitel kontaktuje pověřence, se kterým zkonzultuje další postup.
5) Při kontaktu s pověřencem (případně následně též s dozorovým úřadem) je povinností organizace, co nejpřesněji bezpečnostní incident popsat. Popis bezpečnostního incidentu musí obsahovat alespoň následující:
    a) popis povahy bezpečnostního incidentu (popis co a kde se stalo),
    b) uvedení data a hodiny vzniku či zjištění bezpečnostního incidentu (popis kdy se stalo),
    c) popis kategorií osobních údajů, které jsou bezpečnostním incidentem ohroženy (citlivé osobní údaje, osobní údaje nezletilých apod.),
    d) alespoň přibližný počet subjektů údajů, které mohou být bezpečnostním incidentem ohroženy (nelze-li určit přesně aspoň přibližný počet),
    e) popis případného rizika, které v souvislosti s bezpečnostním incidentem může vzniknout subjektům údajů.
6) Pověřenec (případně pověřenec Moravskoslezského kraje) provede vyhodnocení bezpečnostního incidentu; a to v rozsahu rizika nízkého, středního či vysokého. V případě vyhodnocení bezpečnostního incidentu jako vysoce rizikového, je nutné provést oznámení dozorovému úřadu dle čl. 33 GDPR vždy; v případě vyhodnocení bezpečnostního incidentu jako středně rizikového záleží na okolnostech případu a vyjádření pověřence (event. pověřence Moravskoslezského kraje), zda je nutné dozorovému úřadu incident ohlásit.
7) Ředitel organizace je povinen zajistit evidenci bezpečnostních incidentů v tomto rozsahu:
    a) datum a čas zjištění incidentu,
    b) datum a čas kontaktování pověřence,
    c) popis bezpečnostního incidentu dle odstavce 5 tohoto postupu,
    d) popis důsledků bezpečnostního incidentu,
    e) informace o posouzení rizika posouzení rizika pověřencem, příp. pověřencem Moravskoslezského kraje,
    f) popis případných přijatých opatření v souvislosti s řešením bezpečnostního incidentu,
    g) datum, čas a způsob případného ohlášení bezpečnostního incidentu dozorovému úřadu, případně subjektům osobních údajů dle č. 34 GDPR.
8) V případě, že je v souladu s odst. 6 tohoto postupu nezbytné ohlásit dozorovému úřadu bezpečnostní incident, bude toto ohlášení obsahovat následující:
    a) popis povahy bezpečnostního incidentu (co kdy a kde se stalo),
    b) kontaktní údaje pověřence pro ochranu osobních údajů (jméno, e-mail, telefon),
    c) popis pravděpodobných důsledků bezpečnostního incidentu,
    d) popis opatření, která již byla organizací přijata nebo jsou navržena k přijetí s cílem vyřešit daný bezpečnostní incident.