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: **Střední škola průmyslová a umělecká, Opava, příspěvková organizace**

Datum účinnosti: od 25. 5. 2048

Verze: 05/2018

I.
Obecná ustanovení

1) Tato směrnice o ochraně osobních údajů (dále také „směrnice") upravuje způsob nakládání s osobními údaji, které Střední škola průmyslová a umělecká, Opava, příspěvková organizace (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: Ing. Šárka Komendová
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 Opavě dne 24. 5. 2018

_____

Ing. Vítězslav Doleží, v.r.
ředitel školy
Střední škola průmyslová
a umělecká, Opava, příspěvková
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.

Příloha č. 3

Směrnice o ochraně osobních údajů a jejich nakládání s nimi

Obecná ustanovení

I. Smysl, účel a způsob zpracování přílohy

1. Cílem přílohy je:
   a. konkretizace povinností u jednotlivých hlavních účelů zpracování,
   b. dokumentace technických a organizačních opatření k zajištění ochrany osobních údajů,
   c. dokumentace k řízení rizik.

II. Zásady zpracování osobních údajů

1. Správce při zpracování osobních údajů dodržuje zásady:
   a. zákonnosti, korektnosti a transparentnosti,
   b. účelového omezení,
   c. minimalizace údajů,
   d. přesnosti,
   e. omezeného uložení,
   f. integrity a důvěrnosti.
2. Správce odpovídá za dodržení souladu s výše uvedenými zásadami a je připraven soulad zpracování se zásadami doložit.

III. Kategorie zpracovávaných osobních údajů, účely a právní tituly pro zpracování

1. Jednotlivé kategorie subjektů, jejichž osobní údaje správce zpracovává, jsou stanoveny v příslušných částech této přílohy.
2. Výčet zpracovávaných osobních údajů je zvlášť ve vztahu k jednotlivým kategoriím subjektů stanoven prostřednictvím Záznamů v příloze č. 3 nebo v elektronické podobě.
3. Účely zpracování osobních údajů jsou stanoveny zvlášť ve vztahu k jednotlivým kategoriím subjektů v příslušných částech této přílohy a podrobně v Záznamech.
4. Právní tituly pro zpracování jsou zvlášť ve vztahu k jednotlivým osobním údajům stanoveny prostřednictvím Záznamů.
5. Elektronicky je veden výčet zpracování, u kterého je nutný souhlas subjektu údajů.
6. Součástí této přílohy je vzor pro vedení evidence souhlasů se zpracováním osobních údajů dle článku 3 odst. 3 písmene f) Směrnice.

Část A: Zpracování osobních údajů zaměstnanců

I. Účely zpracování

1. Správce zpracovává osobní údaje osob, se kterými navázal pracovněprávní vztah (zaměstnanci), za účelem:
   a. zajištění personální (pracovněprávní) a platové agendy,
   b. zajištění výkonu činnosti správce,
   c. propagace správce a jeho činnosti,
   d. zajištění bezpečnosti práce, pracovnělékařských služeb, odškodnění pracovních úrazů a nemocí z povolání.

II. Právní tituly pro zpracování

1. Při zpracování osobních údajů zaměstnanců na základě souhlasu [čl. 6 odst. 1 písm. a) GDPR] platí následující pravidla:
   a. souhlas se zpracováním osobních údajů vyžaduje správce od subjektu pouze ve výjimečném případě, kdy pro zpracování neexistuje jiný právní základ [čl. 6 odst. 1 GDPR],
   b. souhlas se zpracováním osobních údajů bude za účelem následného doložení proveden písemně,
   c. souhlas se zpracováním osobních údajů bude vyhotoven na samostatné listině, která nebude součástí jiného smluvního ujednání,
   d. součástí souhlasu bude zejména:
      - určení osobního údaje, s jehož zpracováním dává subjekt souhlas,
      - určení účelu a způsobu zpracování,
      - určení doby, na kterou je souhlas dáván,
      - poučení o možnosti subjektu odvolat souhlas písemným oznámením adresovaným škole nebo pověřenci,
   e. zaměstnanec je při předložení žádosti o souhlas se zpracováním poučen o tom, že není povinen souhlas udělit a případné udělení souhlasu je z jeho strany dobrovolné a svobodné.
2. Při zpracování osobních údajů zaměstnanců na základě plnění smlouvy [čl. 6 odst. 1 písm. b) GDPR] jde o povinnosti založené:
   a. pracovní smlouvou, dohodou o pracovní činnosti nebo dohodou o provedení práce,
   b. jinou smlouvou či dohodou uzavřenou mezi zaměstnancem a zaměstnavatelem (například kvalifikační dohoda, dohoda o odpovědnosti k ochraně hodnot svěřených zaměstnanci k vyúčtování),
   c. kolektivní smlouvou.
3. Při zpracování osobních údajů zaměstnanců pro plnění právní povinnosti správce [čl. 6 odst. 1 písm. c) GDPR] jde o povinnosti založené zejména:
   a. zákoníkem práce, zákonem o zaměstnanosti a dalšími právními předpisy v oblasti pracovního práva,

b. zákonem o specifických zdravotních službách a dalšími předpisy v oblasti pracovnělékařských služeb,

c. zákonem o dani z příjmu a dalšími daňovými předpisy,

d. právními předpisy v oblasti zdravotního, nemocenského a důchodového pojištění,

e. občanským soudním řádem, exekučním řádem a inslovenčním zákonem.

4. Při zpracování osobních údajů zaměstnanců, které je nezbytné pro účely oprávněných zájmů správce či třetí strany správce [čl. 6 odst. 1 písm. f) GDPR] je zaměstnanec při získání údaje poučen o tom, pro jaký oprávněný zájem je zpracování nezbytné. Jde zejména o oprávněné zájmy správce spočívající v:

   a. zajištění bezpečnosti a ochrany zdraví při práci,

   b. zajištění ochrany majetkových zájmů správce,

   c. oprávněném zájmu školy při běžné prezentaci své činnosti a zobrazení historie.

III. Získání údajů a informační povinnost správce

1. Osobní údaje jsou od zaměstnanců získány:

   a. prostřednictvím životopisu zaslaného v rámci výběrového řízení,

   b. v souvislosti s nástupem do práce vyplněním osobního dotazníku zaměstnance,

   c. z předložených dokladů ve vztahu k odborné kvalifikaci pedagogického pracovníka.

2. Za splnění informační povinnosti správce v souvislosti se získáním osobních údajů [čl. 13 odst. 1 a 2 GDPR], tj.

   a. totožnosti a kontaktních údajích správce,

   b. účelech zpracování, pro které jsou osobní údaje určeny,

   c. právním základu pro zpracování,

   d. oprávněných zájmech správce nebo třetí strany, pokud je zpracování osobního údaje založeno na nezbytnosti pro účely těchto oprávněných zájmů [čl. 6 odst. 1 písm. f) GDPR],

   e. případných příjemcích nebo kategorii příjemců osobních údajů,

   f. případném úmyslu správce předat osobní údaje do třetí země nebo mezinárodní organizaci včetně záruk,

   g. době, po kterou budou osobní údaje uloženy, případně o kritériích použitých pro stanovení této doby,

   h. existenci práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, vznést námitku proti zpracování, jakož i práva na přenositelnost údajů,

   i. v případě údajů zpracovávaných na základě souhlasu informaci o existenci práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním,

   j. existenci práva podat stížnost u Úřadu pro ochranu osobních údajů,

k. o skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů,

l. o skutečnosti, že nedochází k automatizovanému rozhodování, včetně profilování,

m. o skutečnosti, že správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu, která bude poskytnuta písemně, odpovídá zaměstnanec personálního útvaru,

3. Informační povinnost v případě, kdy správce hodlá osobní údaj zaměstnance dále zpracovat pro jiný účel, než je účel, pro který byl shromážděn, zajistí zaměstnanec personálního útvaru písemně.

IV. Prostředky zpracování osobních údajů

1. Osobní údaje zaměstnanců jsou zpracovávány:

   a. v listinné podobě. Příslušné listiny jsou uloženy v osobních spisech, které jsou zabezpečeny způsobem uvedeným níže v čl. V části A Směrnice. K osobním spisům mají přístup pouze zaměstnanci personálního útvaru. Při nahlédnutí jiné osoby do osobního spisu podle § 312 odst. 2 zákoníku práce musí být vždy přítomen zaměstnanec personálního útvaru.

V. Technická a organizační opatření k zajištění ochrany osobních údajů

1. Správce při všech úkonech zpracování osobních údajů zaměstnanců všemi dostupnými a vhodnými prostředky chrání zpracovávané osobní údaje před zničením, ztrátou nebo změnou, neoprávněným poskytnutím nebo zpřístupněním.
2. Osobní údaje:

   a. uchovávané v listinné podobě jsou trvale uloženy v uzamykatelných skříních, které se nachází na sekretariátě školy.

   b. uchovávané v elektronické podobě jsou zabezpečeny prostřednictvím informačního systému „Personální kancelář“.

3. Při zabezpečení osobních údajů zaměstnanců zpracovávaných v listinné podobě platí:

   a. K osobním údajům zpracovávaným správcem mají přístup pouze ti zaměstnanci správce, u kterých je tento přístup nezbytný vzhledem k povinnostem, jež plní v pracovněprávním vztahu k správci.

   b. V případě, kdy podle právních předpisů nebo vzhledem k oprávněným zájmům bude muset jiná osoba nahlédnout do některé z listin, dojde k tomu za přítomnosti některého ze zaměstnanců uvedených v předchozím písmenu.

   c. Listiny obsahující osobní údaj ani jejich kopie nesmí být kromě případů stanovených právními předpisy vynášeny z prostor správce ani předávány nepovolaným osobám.

   d. Zaměstnanci při práci s příslušnými listinami dodržují zásadu prázdného stolu. Znamená to, že zaměstnanec má ve fyzické dispozici pouze listiny, které nezbytně potřebuje a se kterými aktuálně pracuje. Opouští-li své pracoviště, nenechává listiny volně přístupné a bezpečně je ukládá.

4. Při zabezpečení osobních údajů zpracovávaných v elektronické podobě platí:
    a. Do elektronického systému mají přístup pouze zaměstnanci výslovně určení ředitelem.
    b. Do elektronického systému lze přistoupit pouze na základě jedinečného přihlašovacího jména a přístupového hesla. Jednotliví zaměstnanci odpovídají za zabezpečení svého přihlašovacího jména a přístupového hesla.
    c. Stanovení přístupových oprávnění jednotlivým zaměstnancům provede ředitel. Přitom dodržuje princip minimálního oprávnění (přidělení pouze takových oprávnění, která jsou nezbytná k plnění povinností tohoto zaměstnance). Počet a rozsah udělených oprávnění bude pravidelně vyhodnocován a v případě potřeby bezodkladně změněn.
    d. Při práci s elektronickou evidencí nesmí zaměstnanci opouštět počítač bez odhlášení, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přístupového hesla. V případě narušení přístupového zabezpečení hesla musí zaměstnanec bezodkladně zajistit jeho změnu.
    e. Ke dni ukončení pracovněprávního vztahu zaměstnance budou veškerá přístupová oprávnění odebrána.
5. Zaměstnanci, kteří mají přístup k osobním údajům, jsou povinni o obsahu těchto údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
6. Zaměstnanci, kteří se podílí na zabezpečení osobních údajů, jsou povinni o bezpečnostních opatřeních přijatých za účelem zajištění ochrany osobních údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
7. Každý zaměstnanec, který je vázán mlčenlivostí o osobních údajích nebo bezpečnostních opatřeních, bude na povinnost mlčenlivosti výslovně upozorněn při seznámení s obsahem směrnice a jejich příloh. Současně budou tito zaměstnanci poučeni o základních právních souvislostech ochrany osobních údajů. Toto upozornění a poučení bude stvrzeno písemným podpisem. Za provedení upozornění a poučení odpovídá ředitel nebo jím pověřená osoba dle článku II odst. 3) Směrnice.
8. Opatření popsaná v tomto článku budou podle potřeby revidována a aktualizována.

VI. Školení zaměstnanců

1. Zaměstnanci budou v souvislosti s přijetím směrnice a jejich příloh hromadně proškolení o základních pravidlech a zásadách zpracování jejich osobních údajů.
2. Školení budou podle potřeby opakována.

VII. Archivace dokumentů obsahující osobní údaje zaměstnanců

1. Po skončení pracovněprávního vztahu jsou příslušné listiny vztahující se k danému zaměstnanci v souladu s právními povinnostmi správce a vzhledem k nezbytnosti zajištění právem chráněných zájmů správce archivovány zpravidla po následující dobu, pokud ve spisovém a skartačním řádu není uvedena doba delší, nezbytně nutná vzhledem k oprávněným zájmům správce:

Pracovněprávní dokumenty, jejichž uschování je nezbytné pro ochranu práv správce v případném soudním sporu (pracovní smlouva, rozvázání pracovního poměru, platový výměr atd.)	4 roky
Dokumenty, které mají charakter účetního dokladu.	10 let
Mzdové listy a účetní záznamy o údajích potřebných pro účely důchodového pojištění.	30 let
Evidenční listy důchodového pojištění.	3 roky

2. Po uplynutí výše uvedených archivačních lhůt budou osobní údaje vymazány a listiny obsahující osobní údaje zlikvidovány.
3. Ostatní listiny a osobní údaje jsou zlikvidovány, resp. vymazány při skončení pracovního poměru.

Část B: Zpracování osobních údajů uchazečů o zaměstnání

I. Účel zpracování

1. Správce zpracovává osobní údaje osob, které se u něj ucházejí o zaměstnání, za účelem efektivního výběru vhodného uchazeče, který odpovídá kvalifikačním a dalším požadavkům stanoveným správcem.

II. Právní tituly pro zpracování

1. Při zpracování osobních údajů uchazečů o zaměstnání na základě souhlasu [čl. 6 odst. 1 písm. a) GDPR]:
   a. souhlas se zpracováním osobních údajů vyžaduje správce od subjektu pouze ve výjimečném případě, kdy pro zpracování neexistuje jiný právní základ [čl. 6 odst. 1 GDPR],
   b. souhlas se zpracováním osobních údajů bude za účelem následného doložení proveden písemně,
   c. souhlas se zpracováním osobních údajů bude vyhotoven na samostatné listině, která nebude součástí jiného smluvního ujednání,
   d. součástí souhlasu bude zejména:
      - určení osobního údaje, s jehož zpracováním dává subjekt souhlas,
      - určení účelu a způsobu zpracování,
      - určení doby, na kterou je souhlas dáván,
      - poučení o možnosti subjektu odvolat souhlas písemným oznámením adresovaným škole nebo pověřenci,
   e. uchazeč je při předložení žádosti o souhlas se zpracováním poučen o tom, že není povinen souhlas udělit a případné udělení souhlasu je z jeho strany dobrovolné a svobodné.
2. Základním právním titulem pro zpracování osobních údajů uchazečů o zaměstnání je provádění kroků směřujících k uzavření pracovní smlouvy na základě žádosti uchazeče (přihlášení do výběrového řízení) [čl. 6 odst. 1 písm. b) GDPR].

III. Získání údajů a prostředky zpracování osobních údajů

1. Osobní údaje uchazečů o zaměstnání jsou získány prostřednictvím:
   a. životopisů zaslaných samotnými uchazeči,
   b. osobního dotazníku uchazeče,
   c. záznamu o průběhu pohovoru.
2. Osobní údaje uchazečů o zaměstnání jsou zpracovávány:
   a. v listinné podobě a jsou uloženy na sekretariátě školy.
3. Za zpracování odpovídá zaměstnanec personálního útvaru.

IV. Výmaz a likvidace

1. Získané osobní údaje uchazečů o zaměstnání jsou vymazány a listiny obsahující tyto osobní údaje zlikvidovány při skončení pracovního poměru.
2. Osobní údaje uchazečů, se kterými byl založen pracovněprávní vztah, jsou dále zpracovávány, pokud jsou nezbytné pro trvání pracovněprávního vztahu, podle části A této přílohy.
3. Osobní údaje neúspěšných uchazečů mohou být dále zpracovány pro účely následného oslovení tohoto uchazeče v dalším výběrovém řízení, pokud s tím uchazeč neprojeví nesouhlas. Osobní údaje budou uchovány po dobu nejvýše po dobu 2 let.

Část C: Zpracování osobních údajů žáků a jejich zákonných zástupců

I. Účely zpracování

1. Správce zpracovává osobní údaje žáků a jejich zákonných zástupců, za účelem:
   a. zajištění výchovy a vzdělávání žáků ve středním vzdělávání, a to v přijímání ke vzdělávání, jeho organizaci a zajištění průběhu v souladu s ustanoveními zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon) a dalších činnostech, které se vzděláváním souvisí,
   b. zajištění výkonu činnosti správce v oblasti výchovy a vzdělávání,
   c. prezentace své výchovně vzdělávací činnosti a zobrazení historie,
   d. zajištění bezpečnosti a ochrany zdraví žáků,
   e. zajištění ochrany majetku.

II. Právní tituly pro zpracování

1. Při zpracování osobních údajů žáků a jejich zákonných zástupců na základě souhlasu [čl. 6 odst. 1 písm. a) GDPR] platí následující pravidla:
   a. souhlas se zpracováním osobních údajů vyžaduje správce od subjektu pouze ve výjimečném případě, kdy pro zpracování neexistuje jiný právní základ [čl. 6 odst. 1 GDPR],
   b. souhlas se zpracováním osobních údajů bude za účelem následného doložení proveden písemně,
   c. souhlas se zpracováním osobních údajů bude vyhotoven na samostatné listině, která nebude součástí jiného smluvního ujednání,
   d. součástí souhlasu bude zejména:
      - určení osobního údaje, s jehož zpracováním dává subjekt souhlas,
      - určení účelu a způsobu zpracování,
      - určení doby, na kterou je souhlas dáván,
      - poučení o možnosti subjektu odvolat souhlas písemným oznámením adresovaným škole nebo pověřenci,
   e. žák nebo jeho zákonný zástupce je při předložení žádosti o souhlas se zpracováním poučen o tom, že není povinen souhlas udělit a případné udělení souhlasu je z jeho strany dobrovolné a svobodné.
2. Při zpracování osobních údajů žáků a jejich zákonných zástupců na základě plnění smlouvy [čl. 6 odst. 1 písm. b) GDPR] jde o povinnosti založené:
   a. přijetím objednávky, přihlášky a plnění smlouvy podle zákona občanského zákoníku.
3. Při zpracování osobních údajů žáků a jejich zákonných zástupců pro plnění právní povinnosti správce [čl. 6 odst. 1 písm. c) GDPR] jde o povinnosti založené zejména:
   a. školským zákonem a dalšími právními předpisy v oblasti výchovy a vzdělávání,
   b. správním řádem a zákonem o svobodném přístupu k informacím.

4. Při zpracování osobních údajů žáků a jejich zákonných zástupců, které je nezbytné pro účely oprávněných zájmů správce či třetí strany správce [čl. 6 odst. 1 písm. f) GDPR] je žák, zákonný zástupce při získání údaje poučen o tom, pro jaký oprávněný zájem je zpracování nezbytné. Jde zejména o oprávněné zájmy správce spočívající v:
    a. oprávněném zájmu školy při běžné prezentaci své činnosti a zobrazení historie,
    b. oprávněném zájmu školy při ochraně majetku,
    c. zajištění bezpečnosti a ochrany zdraví žáků.

III. Získání údajů a informační povinnost správce

1. Osobní údaje jsou od žáků a zákonných zástupců získány zejména:
    a. prostřednictvím zápisu ke vzdělávání nebo podání přihlášky ke vzdělávání,
    b. prostřednictvím podání přihlášky k poskytování školských služeb.
2. Za splnění informační povinnosti správce v souvislosti se získáním osobních údajů [čl. 13 odst. 1 a 2 GDPR] tj.:
    a. totožnosti a kontaktních údajích správce,
    b. účelech zpracování, pro které jsou osobní údaje určeny,
    c. právním základu pro zpracování,
    d. oprávněných zájmech správce nebo třetí strany, pokud je zpracování osobního údaje založeno na nezbytnosti pro účely těchto oprávněných zájmů [čl. 6 odst. 1 písm. f) GDPR],
    e. případných příjemcích nebo kategorii příjemců osobních údajů,
    f. případném úmyslu správce předat osobní údaje do třetí země nebo mezinárodní organizaci včetně záruk,
    g. době, po kterou budou osobní údaje uloženy, případně o kritériích použitých pro stanovení této doby,
    h. existenci práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, vznést námitku proti zpracování, jakož i práva na přenositelnost údajů,
    i. v případě údajů zpracovávaných na základě souhlasu informaci o existenci práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním,
    j. existenci práva podat stížnost u Úřadu pro ochranu osobních údajů,
    k. o skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů,
    l. o skutečnosti, že nedochází k automatizovanému rozhodování, včetně profilování,
    m. o skutečnosti, že správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu, která bude poskytnuta

písemně, odpovídají zaměstnanci v pracovních pozicích dle organizace vzdělávání a poskytování školských služeb.

IV. Prostředky zpracování osobních údajů

1. Osobní údaje žáků a zaměstnanců jsou zpracovávány:
   a. v listinné podobě. Příslušné listiny dle vyhlášky o dokumentaci škol a školských zařízení a dalších právních předpisů, jsou zabezpečeny způsobem uvedeným v čl. V části C této přílohy. K dokumentaci mají přístup pouze pověření zaměstnanci ředitelem školy.
   b. v elektronické databázi Škola online.
2. V případě předávání osobních údajů na základě zákonné žádosti subjektům, např. zřizovateli, ŠPZ, MŠMT, ČŠI, CZVV, zdravotním pojišťovnám, Policii ČR, OSPOD, soudu apod. jsou osobní údaje, zasílány datovou schránkou, doporučeně poštou, případně předány osobně.
3. V případě, kdy je správce povinen zpracovat osobní údaj zvláštní kategorie (zejména údaje o znevýhodnění žáka, údaje o mimořádném nadání, údaje o podpůrných opatřeních poskytovaných žákovi školou, a o závěrech vyšetření uvedených v doporučení školského poradenského zařízení, údaje o zdravotní způsobilosti ke vzdělávání a o zdravotních obtížích, které by mohly mít vliv na průběh vzdělávání), má k osobnímu údaji přístup pouze úzce vymezený okruh zaměstnanců pověřených ředitelem školy, kteří tyto údaje nezbytně potřebují k naplňování výchovně vzdělávacích potřeb žáka.

V. Technická a organizační opatření k zajištění ochrany osobních údajů

1. Správce při všech úkonech zpracování osobních údajů všemi dostupnými a vhodnými prostředky chrání zpracovávané osobní údaje před zničením, ztrátou nebo změnou, neoprávněným poskytnutím nebo zpřístupněním.
2. Osobní údaje:
   a. uchovávané v listinné podobě jsou trvale uloženy v uzamykatelných skříních, které se nachází na sekretariátě školy.
   b. uchovávané v elektronické podobě jsou zabezpečeny prostřednictvím informačního systému Škola online případně informačního systému „Personální kancelář“.
3. Při zabezpečení osobních údajů zpracovávaných v listinné podobě platí:
   a. K osobním údajům žáků a zákonných zástupců zpracovávaným správcem mají přístup pouze ti zaměstnanci správce, u kterých je tento přístup nezbytný vzhledem k povinnostem, jež plní v pracovněprávním vztahu k správci.
   b. V případě, kdy podle právních předpisů nebo vzhledem k oprávněným zájmům bude muset jiná osoba nahlédnout do některé z listin, dojde k tomu za přítomnosti některého z pověřených zaměstnanců ředitelem školy nebo jím jmenovaná odpovědná osoby dle článku II odst. 3) Směrnice.
   c. Listiny obsahující osobní údaj ani jejich kopie nesmí být kromě případů stanovených právními předpisy vynášeny z prostor správce ani předávány nepovolaným osobám.
   d. Zaměstnanci při práci s příslušnými listinami dodržují zásadu prázdného stolu. Znamená to, že zaměstnanec má ve fyzické dispozici pouze listiny, které nezbytně

potřebuje a se kterými aktuálně pracuje. Opouští-li své pracoviště, nenechává listiny volně přístupné a bezpečně je ukládá.

4. Při zabezpečení osobních údajů žáků a zákonných zástupců zpracovávaných v elektronické podobě platí:
   a. Do elektronického systému mají přístup pouze zaměstnanci výslovně určení ředitelem školy, nebo jím jmenované odpovědné osoby dle článku II odst. 3) Směrnice.
   b. Do elektronického systému lze přistoupit pouze na základě jedinečného přihlašovacího jména a přístupového hesla. Jednotliví zaměstnanci odpovídají za zabezpečení svého přihlašovacího jména a přístupového hesla.
   c. Stanovení přístupových oprávnění jednotlivým zaměstnancům provede ředitel školy nebo jím jmenovaná odpovědná osoba dle článku II odst. 3) Směrnice. Přitom dodržuje princip minimálního oprávnění (přidělení pouze takových oprávnění, která jsou nezbytná k plnění povinností tohoto zaměstnance). Počet a rozsah udělených oprávnění bude pravidelně vyhodnocován a v případě potřeby bezodkladně změněn.
   d. Při práci s elektronickou evidencí nesmí zaměstnanci opouštět počítač bez odhlášení, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přístupového hesla. V případě narušení přístupového zabezpečení hesla musí zaměstnanec bezodkladně zajistit jeho změnu.
   e. Ke dni ukončení pracovněprávního vztahu zaměstnance budou veškerá přístupová oprávnění odebrána.
5. Zaměstnanci, kteří mají přístup k osobním údajům žáků a jejich zákonných zástupců, jsou povinni o obsahu těchto údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
6. Zaměstnanci, kteří se podílí na zabezpečení osobních údajů žáků a jejich zákonných zástupců, jsou povinni o bezpečnostních opatřeních přijatých za účelem zajištění ochrany osobních údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
7. Každý zaměstnanec, který je vázán mlčenlivostí o osobních údajích nebo bezpečnostních opatřeních, bude na povinnost mlčenlivosti výslovně upozorněn při seznámení s obsahem této směrnice a jejích příloh. Současně budou tito zaměstnanci poučeni o základních právních souvislostech ochrany osobních údajů. Toto upozornění a poučení bude stvrzeno písemným podpisem. Za provedení upozornění a poučení odpovídá ředitel školy nebo jím jmenovaná odpovědná osoba dle článku II odst. 3) Směrnice.
8. Opatření popsaná v tomto článku budou podle potřeby revidována a aktualizována.

VI. Školení zaměstnanců

1. Zaměstnanci budou v souvislosti s přijetím směrnice a jejích příloh hromadně proškolení o základních pravidlech a zásadách zpracování osobních údajů.
2. Školení budou opakována podle potřeby, zejména s přihlédnutím k počtu nově nastupujících zaměstnanců.

VII. Archivace dokumentů obsahující osobní údaje žáků a jejich zákonných zástupců

1. Po skončení vzdělávání jsou příslušné listiny vztahující se k danému žákovi a jeho zákonnému zástupci v souladu s právními povinnostmi správce a vzhledem k nezbytnosti zajištění právem chráněných zájmů správce archivovány po dobu uvedenou ve spisovém a skartačním řádu a v Záznamech o zpracování.
2. Po uplynutí archivačních lhůt budou osobní údaje z informačních systémů vymazány a listiny obsahující osobní údaje zlikvidovány, pokud nejde o archiválie podle bodu 16 přílohy č. 2, zákona č. 499/2004 Sb. o archivnictví a spisové službě.
3. Ostatní listiny a osobní údaje jsou zlikvidovány, resp. vymazány při skončení výchovy a vzdělávání žáka.

Část D: Zpracování osobních údajů dodavatelů, smluvních partnerů v hlavní i doplňkové činnosti školy

I. Účely zpracování

1. Správce zpracovává osobní údaje osob, se kterými navázal smluvní vztahy (dodavatelé, partneři), zejména za účelem:
   a. zajištění provozu školy ve vztahu k energiím a údržbě,
   b. zajištění výchovy a vzdělávání ve smyslu zajištění učebnic, učebních pomůcek a programového a dalšího vybavení pro výchovu a vzdělávání,
   c. zajištění dalších činností ve své hlavní a doplňkové činnosti,
   d. zajištění vedení účetnictví.

II. Právní tituly pro zpracování

1. Při zpracování osobních údajů dodavatelů, smluvních partnerů v hlavní i doplňkové činnosti školy na základě plnění smlouvy [čl. 6 odst. 1 písm. b) GDPR] jde o povinnosti založené:
   a. přijetím objednávky, přihlášky nebo plněním smlouvy.
2. Při zpracování osobních údajů zaměstnanců pro plnění právní povinnosti správce [čl. 6 odst. 1 písm. c) GDPR] jde o povinnosti založené zejména:
   a. zákonem o účetnictví, zákonem o rozpočtových pravidlech územních rozpočtů,
   b. zákonem o dani z přidané hodnoty, spotřební dani, dani z příjmu a dalšími daňovými předpisy.
3. Při zpracování osobních údajů zaměstnanců, které je nezbytné pro účely oprávněných zájmů správce či třetí strany správce [čl. 6 odst. 1 písm. f) GDPR] je zaměstnanec při získání údaje poučen o tom, pro jaký oprávněný zájem je zpracování nezbytné. Jde zejména o oprávněné zájmy správce spočívající v:
   a. zajištění ochrany majetkových zájmů správce.

III. Získání údajů a informační povinnost správce

1. Osobní údaje jsou od dodavatelů a partnerů získány:
   a. prostřednictvím smlouvy nebo návrhu uzavření smlouvy,
   b. v přihlášce nebo objednávce služby.

IV. Prostředky zpracování osobních údajů

1. Osobní údaje dodavatelů a partnerů jsou zpracovávány:
   a. v listinné podobě. Příslušné listiny jsou uloženy v účetních spisech a smluvních ujednáních, které jsou zabezpečeny způsobem uvedeným níže v čl. V části D přílohy. K osobním spisům mají přístup pouze zaměstnanci ekonomického úseku. Při nahlédnutí jiné osoby do účetních spisů a smluvních ujednání musí být vždy přítomen zaměstnanec ekonomického úseku.

b. v elektronické databázi „Gordic“.

V. Technická a organizační opatření k zajištění ochrany osobních údajů dodavatelů a partnerů

1. Správce při všech úkonech zpracování osobních údajů dodavatelů a partnerů všemi dostupnými a vhodnými prostředky chrání zpracovávané osobní údaje před zničením, ztrátou nebo změnou, neoprávněným poskytnutím nebo zpřístupněním.
2. Osobní údaje:
   a. uchovávané v listinné podobě jsou trvale uloženy v uzamykatelných skříních, které se nachází v kanceláři ekonomického úseku školy.
   b. uchovávané v elektronické podobě jsou zabezpečeny prostřednictvím informačního systému „Gordic“.
3. Při zabezpečení osobních údajů dodavatelů a partnerů zpracovávaných v listinné podobě platí:
   a. K osobním údajům zpracovávaným správcem mají přístup pouze ti zaměstnanci správce, u kterých je tento přístup nezbytný vzhledem k povinnostem, jež plní v pracovněprávním vztahu k správci.
   b. V případě, kdy podle právních předpisů nebo vzhledem k oprávněným zájmům bude muset jiná osoba nahlédnout do některé z listin, dojde k tomu za přítomnosti některého ze zaměstnanců uvedených v předchozím písmenu.
   c. Listiny obsahující osobní údaj ani jejich kopie nesmí být kromě případů stanovených právními předpisy vynášeny z prostor správce ani předávány nepovolaným osobám.
   d. Zaměstnanci při práci s příslušnými listinami dodržují zásadu prázdného stolu. Znamená to, že zaměstnanec má ve fyzické dispozici pouze listiny, které nezbytně potřebuje a se kterými aktuálně pracuje. Opouští-li své pracoviště, nenechává listiny volně přístupné a bezpečně je ukládá.
4. Při zabezpečení osobních údajů zpracovávaných v elektronické podobě platí:
   a. Do elektronického systému mají přístup pouze zaměstnanci výslovně určení ředitelem.
   b. Do elektronického systému lze přistoupit pouze na základě jedinečného přihlašovacího jména a přístupového hesla. Jednotliví zaměstnanci odpovídají za zabezpečení svého přihlašovacího jména a přístupového hesla.
   c. Stanovení přístupových oprávnění jednotlivým zaměstnancům provede ředitel. Přitom dodržuje princip minimálního oprávnění (přidělení pouze takových oprávnění, která jsou nezbytná k plnění povinností tohoto zaměstnance). Počet a rozsah udělených oprávnění bude pravidelně vyhodnocován a v případě potřeby bezodkladně změněn.
   d. Při práci s elektronickou evidencí nesmí zaměstnanci opouštět počítač bez odhlášení, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přístupového hesla. V případě narušení přístupového zabezpečení hesla musí zaměstnanec bezodkladně zajistit jeho změnu.

e. Ke dni ukončení pracovněprávního vztahu zaměstnance budou veškerá přístupová oprávnění odebrána.

5. Zaměstnanci, kteří mají přístup k osobním údajům, jsou povinni o obsahu těchto údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
6. Zaměstnanci, kteří se podílí na zabezpečení osobních údajů, jsou povinni o bezpečnostních opatřeních přijatých za účelem zajištění ochrany osobních údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
7. Každý zaměstnanec, který je vázán mlčenlivostí o osobních údajích nebo bezpečnostních opatřeních, bude na povinnost mlčenlivosti výslovně upozorněn při seznámení s obsahem směrnice a jejích příloh. Současně budou tito zaměstnanci poučeni o základních právních souvislostech ochrany osobních údajů. Toto upozornění a poučení bude stvrzeno písemným podpisem. Za provedení upozornění a poučení odpovídá ředitel nebo jím pověřená osoba dle článku II odst. 3) Směrnice.
8. Opatření popsaná v tomto článku budou podle potřeby revidována a aktualizována.

VI. Školení zaměstnanců

1. Zaměstnanci budou v souvislosti s přijetím směrnice a jejích příloh hromadně proškolení o základních pravidlech a zásadách zpracování jejich osobních údajů.
2. Školení budou podle potřeby opakována.

VII. Archivace dokumentů obsahující osobní údaje dodavatelů a partnerů

1. Po skončení smluvního vztahu jsou příslušné listiny vztahující se k danému smluvnímu vztahu v souladu s právními povinnostmi správce a vzhledem k nezbytnosti zajištění právem chráněných zájmů správce archivovány zpravidla po následující dobu, pokud ve spisovém a skartačním řádu není uvedena doba delší, nezbytně nutná vzhledem k oprávněným zájmům správce:

Pro účely vedení účetnictví: účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh	5 let
Účetní závěrka a výroční zpráva	10 let
Daňové doklady dle zákona o dani z přidané hodnoty	10 let

2. Po uplynutí výše uvedených archivačních lhůt budou osobní údaje vymazány a listiny obsahující osobní údaje zlikvidovány.
3. Ostatní listiny a osobní údaje nepodléhající zákonným lhůtám archivace jsou zlikvidovány, resp. vymazány při skončení smluvního vztahu.

Část E: Monitoring objektů, kamerové systémy

I. Účel zpracování

1. Správce zpracovává osobní údaje žáků, zaměstnanců a příležitostně vstupujících osob do monitorovaného prostoru (dodavatelé, návštěvy apod.) v rozsahu podoba a obrazové informace o chování a jednání zaznamenaných osob za účelem ochrany majetku správce, žáků a zaměstnanců a zajištění jejich bezpečnosti a ochrany zdraví.

II. Právní tituly pro zpracování

1. Základním právním titulem je zpracování oprávněných zájmů příslušného správce [čl. 6 odst. 1 písm. f) GDPR].
2. Při zpracování osobních údajů, které je nezbytné pro účely oprávněných zájmů správce [čl. 6 odst. 1 písm. f) GDPR] je subjekt údajů informován v místech před záběrem sledovaného prostoru o užití kamerového systému, a o tom, kdo jej provozuje, a o způsobu uplatnění práv subjektu údajů (informační tabulka s piktogramem kamery, odkaz na webovou stránku s podrobnými údaji o ochraně osobních údajů, telefonní spojení, adresa správce).
3. Zaměstnanci jsou při zpracování osobních údajů kamerovým systémem přímo informováni o místech, rozsahu a způsobu monitorování prostor s kamerovým záznamem a zdůvodnění jeho účelu v souladu s ustanovením § 316 odst. 2) a 3) zákona č. 262/2006 Sb. v rozsahu:
    a. prostory jsou monitorovány pouze za účelem ochrany majetku správce, žáků a zaměstnanců a zajištění jejich bezpečnosti a ochrany zdraví,
    b. monitorovány jsou pouze prostory, kde nedochází k výchovně vzdělávací činnosti nebo výkonu práce,
    c. monitorovány jsou prostory přístupů do budov, prostory před šatnami žáků, vnitřní areály školy a parkoviště školy.

III. Získání údajů a prostředky zpracování osobních údajů

1. Osobní údaje žáků, zaměstnanců a příležitostně vstupujících osob do monitorovaného prostoru (dodavatelé, návštěvy apod.) jsou získány prostřednictvím záznamu z kamerového systému uložený na paměťovém médiu, za zpracování odpovídá zaměstnanec ICT správce.

IV. Technická a organizační opatření k zajištění ochrany osobních údajů žáků, zaměstnanců a příležitostně vstupujících osob do monitorovaného prostoru (dodavatelé, návštěvy apod.)

1. Správce při všech úkonech zpracování osobních údajů dodavatelů a partnerů všemi dostupnými a vhodnými prostředky chrání zpracovávané osobní údaje před zničením, ztrátou nebo změnou, neoprávněným poskytnutím nebo zpřístupněním.
2. Správce udržuje dokumentaci k instalaci a provozu kamer a přijatým technickoorganizačním opatřením v aktuálním stavu zejména přijatá opatření k eliminaci hrozeb:
    a. neoprávněného přístupu k prostředkům kamerového systému,

b. neoprávněného přístupu ke kamerovým záznamům,
c. neoprávněného čtení, kopírování, přenosu, úprav nebo vymazání kamerových záznamů.

3. Osobní údaje uchovávané v elektronické podobě jsou zabezpečeny prostřednictvím bezpečnostního krytu, tj. řízeného přístupu k datům, školením oprávněných osob, vedení záznamů o předání nahrávek oprávněným orgánům a osobám.
4. Při zabezpečení osobních údajů zpracovávaných v kamerových systémech dále platí:
   a. Přístup k databázi se záznamem má přístup pouze zaměstnanec výslovně určený ředitelem, tj. správce budov.
   b. K manipulaci a nastavování kamerového systému jsou určeni zaměstnanci výslovně určeni ředitelem školy, tj. ICT správce.
   c. K záznamům z kamerového systému lze přistoupit pouze na základě jedinečného přihlašovacího jména a přístupového hesla. Zaměstnanec uvedený v odst. 4. bodu a. odpovídá za zabezpečení svého přihlašovacího jména a přístupového hesla.
   d. Při manipulaci se záznamem nesmí zaměstnanec opouštět počítač bez vypnutí záznamu a bez odhlášení z počítače, nemůže nechat nahlížet žádnou jinou osobu a musí chránit utajení přístupového hesla. V případě narušení přístupového zabezpečení hesla musí zaměstnanec bezodkladně zajistit jeho změnu.
   e. Ke dni ukončení pracovněprávního vztahu zaměstnance budou veškerá přístupová oprávnění odebrána.
5. Zaměstnanci, kteří mají přístup k záznamům osobních údajů, jsou povinni o obsahu těchto údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
6. Zaměstnanci, kteří se podílí na zabezpečení záznamů osobních údajů, jsou povinni o bezpečnostních opatřeních přijatých za účelem zajištění ochrany osobních údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.
7. Každý zaměstnanec, který je vázán mlčenlivostí o osobních údajích nebo bezpečnostních opatřeních, bude na povinnost mlčenlivosti výslovně upozorněn při seznámení s obsahem směrnice a jejích příloh. Současně budou tito oprávnění zaměstnanci poučeni o právních souvislostech ochrany osobních údajů u záznamových zařízení. Toto upozornění a poučení bude stvrzeno písemným podpisem. Za provedení upozornění a poučení odpovídá ředitel nebo jím pověřená osoba dle článku II odst. 3) Směrnice.
8. Opatření popsaná v tomto bodu budou periodicky revidována a aktualizována.

V. Výmaz a likvidace

1. Získané osobní údaje jsou soustavně přemazávány v úložním médiu cca v 3. denní smyčce.
2. Zaznamenané osobní údaje jsou přemazávány v období školních prázdnin cca v 10. denní smyčce.
3. Záznam zachyceného incidentu je uchován po dobu nezbytnou pro projednání případu.

Část G: ICT bezpečnost při zpracování osobních údajů

I. Účel zpracování

Správce za účelem zajištění vzdělávání, zajištění personální a platové agendy související s existencí pracovněprávních vztahů a dalších souvisejících činností hlavní i doplňkové činnosti školy provádí operace s osobními údaji uloženými v elektronické podobě ve smyslu jejich shromažďování, zpřístupňování, úprav nebo pozměňování, vyhledávání, používání, třídění, předávání, šíření, zveřejňování, uchovávání a skartace.

II. Technická a organizační opatření k zajištění ochrany osobních údajů při jejich elektronickém zpracování

Smyslem uvedených organizačních a technických opatření je 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, zajistit úroveň zabezpečení odpovídající jednotlivým rizikům zpracování osobních údajů ve škole, a dále zajistit důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, dostát schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů, zajistit proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Nastavení a posuzování technických a organizačních opatření je vedeno zejména se zřetelem na rizika náhodného nebo protiprávního zničení, ztráty, pozměňování, neoprávněného zpřístupnění.

Všichni pedagogičtí i nepedagogičtí pracovníci, kteří přicházejí do styku s výpočetní technikou, ať už se podílejí nebo nepodílejí na zpracování osobních údajů v elektronických a informačních systémech školy, jsou povinni dodržovat níže uvedená opatření.

1. Organizace

a. Ředitel školy ustanoví ICT správce a role případných dalších administrátorů.
b. ICT správce navrhne řediteli školy ke schválení přidělení administrátorských účtů a jejich úroveň.
c. Ředitel školy dále stanoví odpovědné osoby za hlavní účely zpracování osobních údajů v rozsahu:
   - vedoucí zaměstnanec,
   - osoba odpovědná za operace (zápis, oprava, výmaz apod.) s osobními daty v elektronických systémech,
   - osoba zodpovědná za ICT bezpečnost u informačních systémů a aplikací.
d. Ředitel školy nebo jím pověřená osoba dle článku II odst. 3) Směrnice stanoví úrovně přístupů pedagogických pracovníků do informačního systému a matriky žáků.

2. Zásady a pravidla bezpečnosti elektronického zpracování pro zaměstnance

2.1. Hardware

a. Udržují svěřenou techniku v čistotě, v ochraně před vlhkem, prachem a možným nebezpečím politím tekutinou.

b. Omezují zbytečné restarty po pádu aplikací.

c. Neumisťují svěřenou techniku na nevhodná místa např. třesoucí se podklad, parapety oken apod.

d. Průběžně monitorují chod větrání pracovních stanic.

e. Za chodu nevypínají počítače vytažením ze silové sítě, ale nejdříve použijí k vypnutí systémovou nabídku.

f. V případě hlášených bouřek před odchodem ze směny vypínají počítače i ze silové sítě.

2.2. Software

a. Jsou povinni dodržovat stav legálně instalovaného software a dodržovat jej po celou dobu trvání pracovněprávního vztahu, a to na všech počítačích, nosičích dat a pracovištích zaměstnavatele, se kterými přicházejí do styku.

2.3. Antivirový a aktualizační systém

a. Kontrolují funkčnost a aktuálnost zavedeného antivirového řešení na přidělené technice, hlášení antivirové aplikace sdělují příslušnému správci ICT.

b. Konzultují záchyt hrozeb antivirovým programem s příslušným správcem ICT.

c. Strpí aktualizační procesy operačních systémů s oprávněním přednosti před pracovním nasazením stanic a systémů.

2.4. Internet

a. V Internetu si počínají obezřetně, nikdy nestahují z neznámých webů hudbu, filmy, hry, software, nenavštěvuji rizikové stránky.

b. Mohou používat Internet k osobním účelům jen v minimální míře a za předpokladu, že tím není narušeno plnění pracovních úkolů.

c. Při otevírání internetové stránky se vždy přesvědčí, že souhlasí její doména s obsahem.

2.5. Přenosné disky počítače a datová média

a. K počítačům a školním sítím nepřipojují soukromá datová media, ledaže příslušný správce ICT nestanoví jinak.

b. Po ukončení práce se školními datovými médii, zejména médii s osobními údaji a zálohami informačních systémů nebo kancelářských aplikaci (Word, Excel), tato odpojí a uzamykají, v případě médií se zálohami osobních údajů z informačních systémů na místě určeném správcem ICT.

c. Zálohy osobních údajů na přenosných médiích z informačních systémů nevynášejí mimo pracoviště zaměstnavatele, ledaže by šlo o pracovní povinnosti výslovně určené ředitelem školy nebo s vědomím jím pověřené osoby dle článku II odst. 3) Směrnice.

d. Přidělené školní přenosné počítače (notebooky) mimo pracoviště zaměstnavatele nenechávají bez dozoru, nepřipojují se ke školním ani školním cloudovým službám v prostředí veřejných sítí.

e. Ztrátu bezodkladně hlásí svému přímému nadřízenému a příslušnému správci ICT.

2.6. Zálohování dat

a. Nesou odpovědnost za zálohování dat na přidělených lokálních desktopových i přenosných počítačích a svěřených zálohovacích médiích.
b. Konzultují se správcem ICT potřebný rozsah, četnost a způsob zálohování.

2.7. Hesla

a. Pokud jim role umožňuje tvorbu vlastního hesla, dodržují jeho sílu dle stanovených pravidel pro tvorbu hesel ICT správcem.
b. Přidělené přístupové heslo nikomu nesdělují, ani si jej nezapisují a nepoužívají heslo dále pro přístupy k jiným službám, sítím apod.
c. Při přihlášení k aplikacím a systémům se chovají tak, aby nebylo možné zápis hesla sledovat dalšími osobami.
d. V případě že heslo bylo zveřejněno, heslo neprodleně změní.
e. V případě podezření na zneužití, heslo neprodleně změní a uvedenou skutečnost bezodkladně ohlásí příslušnému správci ICT a svému přímému nadřízenému.
f. Jsou si vědomi, že ke dni ukončení pracovněprávního vztahu jim budou veškerá přístupová oprávnění odebrána.

2.8. Elektronická pošta

a. Zvlášť velký pozor dávají na příchozí zprávy, nikdy neotevírají zprávy z neznámých zdrojů, ani na ně neodpovídají.
b. Pokud posílají dokumenty s osobními údaji ze školy elektronickou poštou např. v pdf formátu, vždy je chráním heslem.
c. Pokud posílají soubory dokumentů elektronickou poštou používají archivní soubory *.zip, *.rar chráněné heslem.
d. Heslo k otevření dokumentu nebo souborů nikdy neposílají v těle zprávy, ale jiným komunikačním kanálem.
e. Pokud posílají hromadnou zprávu např. rodičům, zpráva nikdy neobsahuje osobní údaje a kontakty adresátů v řádku „Kopie“.
f. I když mají nastaveno v elektronické poště šifrované připojení, jsou si vědomi, že u adresáta tomu tak nemusí být.
g. Jsou si vědomi, že pokud stahuji poštu do svého počítače, zprávy s osobními údaji zůstávají i na hostovaném poštovním serveru.
h. Jsou si vědomi, že je zakázáno přeposílání zpráv s osobními údaji na soukromé e-adresy nebo mobilní telefony.
i. Jsou si vědomi, že složky doručená a odeslaná pošta obsahují zprávy s osobními údaji, proto i zde uplatňuji pravidlo „čistého stolu“.

2.9. Tiskárny, kopírky

a. Při tisku osobních údajů na sdílené tiskárně, se vždy přesvědčí, že jsou vytištěny a odebrány všechny požadované strany tiskové sestavy.
b. Při kopírování na sdílené kopírce se vždy se přesvědčí, že originál nezůstal uvnitř skeneru.

2.10. Další organizační pokyny

a. Při krátkodobém opuštění svého pracoviště v pracovní době se odhlásí z počítače nebo uzamknou pracovní plochu.
b. Při odchodu na konci směny vypínají počítač, pouze u počítačů, kde se předpokládá nonstop provoz se odhlašují ze svého profilu.
c. Zaměstnanci, kteří mají přístup k záznamům osobních údajů, jsou povinni o obsahu těchto údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.

2.11. Ohlašování případů porušení zabezpečení osobních údajů, řešení incidentu

a. Při incidentu, který by měl nebo mohl mít vliv na náhodné nebo protiprávní zničení, ztrátu, pozměnění, neoprávněné zpřístupnění osobních údajů nejprve dle svých možností a rolí učiní opatření k zábraně eskalace incidentu.
b. Bezodkladně oznámí jakékoliv narušení zabezpečení osobních údajů, které by mělo za následek jejich náhodné nebo protiprávní zničení, ztrátu, pozměnění, neoprávněné zpřístupnění, svému nadřízenému vedoucímu zaměstnanci a správci ICT.
c. Vedoucí zaměstnanec o události bezodkladně informuje pověřence pro ochranu osobních údajů a ředitele školy.
d. Ředitel školy a pověřenec pro ochranu osobních údajů postupuje dále dle Přílohy č. 2 Směrnice, Postup nahlášení bezpečnostního incidentu dle čl. 33 GDPR.

3. Zásady a pravidla bezpečnosti elektronického zpracování pro správce ICT

3.1. Správci ICT jsou podřízeni všichni administrátoři správy školních sítí a informačních aplikací, webových stránek včetně externích smluvních správců. Jednotlivé role administrátorů jsou popsány v Technickém listu správy ICT ve škole.

3.2. Správce ICT je odpovědný za dodržování bezpečnostních pravidel při zpracovávání a ochraně osobních údajů v počítačových sítích a výpočetní technice organizace.

3.3. Spolupracuje s pověřencem pro ochranu osobních údajů při analýze rizik a tvorbě preventivních opatření.

3.4. V případě incidentu správce ICT bezodkladně učiní opatření, která zabrání jeho další eskalaci a opatření k minimalizaci dopadu.

3.5. O incidentu a jeho rozsahu neprodleně informuje ředitele školy a pověřence pro ochranu osobních údajů.

3.6. Vede provozní deník se záznamy zásadních událostí, jejich popisu, řešení a přijatých opatření.

3.7. Poskytuje zaměstnancům technickou i metodickou pomoc při užívání přidělené výpočetní techniky.

3.8. Zodpovídá za nastavení bezpečnostních opatření v rámci školních sítí a užívání informačních systémů a aplikací tak, aby bylo minimalizováno riziko neoprávněných přístupů.

3.9. Zodpovídá za nastavení uživatelských oprávnění a sílu hesel přidělených zaměstnancům dle stanovených rolí ředitelem nebo školy jím pověřené osoby dle článku II odst. 3) Směrnice do počítačové sítě a aplikací.

3.10. Stanovuje náročnost stupně fyzické bezpečnosti serverů a datových úložišť v prostorách školy a přístup administrátorů případně dalších zaměstnanců. Stav popisuje v Technickém listu správy ICT.

3.11. Zodpovídá za aktivní a aktuální antivirový a antimalwarový software na serverech a pracovních stanicích.

3.12. Zodpovídá za stanovení a plnění plánu zálohování v datových úložištích a na lokálních stanicích, ve kterých jsou umístěny aplikace s osobními údaji. Popisuje a aktualizuje zálohovací plán v Technickém listu správy ICT.

3.13. Rozhoduje o způsobu ochrany dat na discích a paměťových médiích v případě oprav nebo servisu výpočetní techniky.

3.14. Zodpovídá za výmaz nebo likvidaci dat z disků a paměťových médií v případě jejich vyřazení, ukončení provozu.

3.15. Provádí kontrolu síťového provozu, logování přístupu uživatelů do aplikací a informačních systémů vhodnými technickými prostředky.

3.16. ICT správce a administrátoři jsou povinni o bezpečnostních opatřeních přijatých za účelem zajištění ochrany osobních údajů zachovávat mlčenlivost, a to i po skončení jejich pracovněprávního vztahu.

3.17. ICT správce a administrátoři jsou vázáni mlčenlivostí o osobních údajích nebo bezpečnostních opatřeních. Současně budou poučeni o právních souvislostech ochrany osobních údajů u záznamových zařízení. Toto upozornění a poučení bude stvrzeno písemným podpisem. Za provedení upozornění a poučení odpovídá ředitel nebo jím pověřená osoba dle článku II odst. 3) Směrnice.

3.18. Externí smluvní administrátoři mají vždy uzavřenou smlouvu nebo dodatek smlouvy (dle poskytnuté metodiky zřizovatelem), ve kterém se zavazují poskytnout dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR a aby byla zajištěna ochrana práv subjektu údajů.

Část H: Řízení a analýza rizik

Škola provádí analýzu rizik v souladu s ustanovením čl. 24 a 32 GDPR.P

Cílem analýzy rizik je zjistit jakým hrozbám je škola ve vztahu ke zpracovávání osobních údajů vystavena, do jaké míry jsou zpracovávané osobní údaje (aktiva) vůči těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba zneužije některou zranitelnost a s jakým dopadem.

Škola zabezpečí nastavení úrovně technických a organizačních opatření v jednotlivých oblastech fyzické, technické, personální (organizační) a administrativní bezpečnosti v úrovních 1 až 2, a to s přihlédnutím k jednotlivým hlavním účelům zpracování jejich rozsahu a možným dopadům na práva subjektů údajů.

Pojmy:

- **Aktivum** znamená pro účely této analýzy zejména vše, co by mělo být odpovídajícím způsobem chráněno ve vztahu ke zpracování osobních údajů
- **Důvěrnost** je nezbytná úroveň míry utajení při zpracování dat a prevence neoprávněného přístupu, a to jak po dobu uchovávání dat v systémech, tak při jejich přenosu nebo po předávání zpracovatelům a dalším adresátům
- **Integrita** znamená zajištění správnosti a úplnosti dat
- **Dostupnost** zajištění dostupnosti dat pro oprávněné osoby v okamžiku potřeby
- **Dopad** je vznik škody v důsledku působení hrozby
- **Hrozba** je jakákoliv událost ohrožující bezpečnost
- **Zranitelnost** je vlastností aktiva, respektive jeho slabé místo, která může být zneužito hrozbou
- **Riziko** je pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti
- **Opatření** snižuje zranitelnost, chrání aktivum před hrozbou
- **Incident** (narušení) je situace, kdy došlo k narušení důvěrnosti, integrity nebo dostupnosti v důsledku překonání bezpečnostních opatření
- **Počty subjektů údajů ve zpracování** znamená průměrný počet subjektů v jednotlivých zpracováních v čase zpracování (zpravidla 1 rok)

Metodika:

- K analýze rizik byla použita metodika vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Nutno zde zdůraznit, že pro zadavatele analýzy (školy) není tato vyhláška příslušná, proto jednotlivé použité části vyhlášky, zejména její přílohy, mohly být, a byly upraveny pro účely této analýzy.

Hodnocení a úrovně důležitosti aktiv (jednotlivých zpracování)

- Pro hodnocení důležitosti aktiv jsou použity stupnice o čtyřech úrovních
- Pro výpočet hodnoty jednotlivých zpracování je použit součtový algoritmus
- Hodnota zpracování = Důvěrnost + Integrita + Dostupnost + Počet subjektů / 4

Stupnice pro hodnocení důvěrnosti			
Úroveň	**Popis**	**Ochrana**	**Stupeň**
Nízká	Osobní údaje jsou veřejně přístupné (např. Školský rejstřík, zákon č. 106/1999 Sb. apod.) Narušení nemá dopad na subjekty osobních údajů.	Není vyžadována žádná ochrana.	**1**
Střední	Osobní údaje nejsou veřejně přístupné, neobsahují osobní údaje uvedené ve zvláštní kategorii osobních údajů.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.	**2**
Vysoká	Osobní údaje nejsou veřejně přístupné, obsahují některé údaje ze zvláštní kategorie osobních údajů, např. nepřímé údaje o zdravotním stavu (doporučení ŠPZ, výsledky lékařských prohlídek pro pracovněprávní vztahy apod.).	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Přenosy informací vnější komunikační sítě jsou chráněny kryptografickými prostředky.	**3**
Kritická	Osobní údaje nejsou veřejně přístupné, obsahují údaje z kategorie zvláštních osobních údajů (odbory, náboženství, zdravotní stav, biometrické údaje atd.).	Pro ochranu důvěrnosti je požadována evidence osob, které k datům přistoupily, metody ochrany zneužití ze strany administrátorů. Přenosy jsou chráněny pomocí kryptografických prostředků.	**4**

Stupnice pro hodnocení integrity			
Úroveň	**Popis**	**Ochrana**	**Stupeň**
Nízká	Zpracování nevyžadují ochranu z hlediska integrity. Narušení nemá dopad na oprávněné zájmy správce, zpracovatele ani subjekty osobních údajů.	Není vyžadována žádná ochrana.	**1**
Střední	Zpracování může vyžadovat ochranu i z hlediska integrity. Narušení může mít dopad na oprávněné zájmy správce, zpracovatele nebo subjekty osobních údajů.	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).	**2**
Vysoká	Zpracování vyžaduje ochranu z hlediska integrity. Narušení vede k poškození oprávněných zájmů správce, zpracovatele nebo subjektů osobních údajů.	Pro ochranu integrity jsou využívány speciální prostředky. Přenosy informací vnější komunikační síti jsou chráněny kryptografickými prostředky.	**3**
Kritická	Zpracování vyžaduje ochranu z hlediska integrity. Narušení vede k velmi vážnému poškození oprávněných zájmů správce, zpracovatele nebo subjektů osobních údajů.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (digitální podpis, datová schránka).	**4**

Stupnice pro hodnocení dostupnosti			
Úroveň	**Popis**	**Ochrana**	**Stupeň**
Nízká	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období.	Pro ochranu je postačující pravidelné zálohování.	**1**
Střední	Narušení dostupnosti by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zpracování u správce nebo zpracovatele.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	**2**
Vysoká	Narušení dostupnosti by nemělo překročit dobu několika hodin. Jakýkoliv výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zpracování u správce nebo zpracovatele.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova služeb může být podmíněna zásahy obsluhy.	**3**
Kritická	Narušení dostupnosti není přípustné, a i krátkodobá nedostupnost vede k vážnému ohrožení zpracování u správce nebo zpracovatele.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova je krátkodobá a automatizovaná.	**4**

Počty subjektů údajů ve zpracování		
Popis		**Stupeň**
Počet subjektů údajů v jednotlivých scénářích zpracování	1 až 500	**1**
	501 až 1 000	**2**
	1 001 až 2 000	**3**
	2 001 a více	**4**

1.1. Hodnocení rizik (jednotlivých zpracování)

- Hodnocení rizik je vyjádřeno jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost
- Pro hodnocení rizik je použita stupnice o čtyřech úrovních s určením míry rizika na 2 desetinná místa v rozpětí 1 až 4
- Pro výpočet hodnoty jednotlivých zpracování je použit součtový algoritmus

Stupnice pro hodnocení dopadů		
Úroveň	**Popis**	**Stupeň**
Nízká	Dopad je v omezeném časovém období a malého rozsahu, zasahující pouze jednotlivá zpracování, bez vlivu na práva subjektů údajů.	**1**
Střední	Dopad je v omezeném časovém období a omezeného rozsahu, zasahující jednotlivé skupiny zpracování, může mít vliv na práva subjektů údajů.	**2**

Vysoká	Dopad je omezeného rozsahu, zasahující jednotlivé IT systémy zpracování, vykazující i případné finanční nebo materiální ztráty správce nebo zpracovatele a dále s dopadem do práv subjektů údajů.	**3**
Kritická	Dopad je plošný, rozsahem katastrofický, zasahující kompletní zpracování a vykazující i značné finanční nebo materiální ztráty správce nebo zpracovatele a mající zásadní vliv na práva subjektů údajů.	**4**

Stupnice pro hodnocení hrozeb		
Úroveň	**Popis**	**Stupeň**
Nízká	Hrozba neexistuje nebo je málo pravděpodobná.	**1**
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 do 5 let.	**2**
Vysoká	Hrozba je pravděpodobná až velni pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	**3**
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	**4**

Stupnice pro hodnocení zranitelnosti		
Úroveň	**Popis**	**Stupeň**
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, která jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.	**1**
Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.	**2**
Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.	**3**
Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.	**4**

Stupnice pro hodnocení rizik		
Úroveň	**Popis**	**Hodnota (H)**
Nízká	Riziko je považováno za přijatelné.	**1,00 až 2,00**
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v	**2,01 až 2,50**

	případě vyšší náročnosti opatření je riziko přijatelné.	
Vysoká	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	**2,51 až 3,00**
Kritická	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	**3,01 až 4,00**

1.2. Hrozby a hodnocení opatření k zabezpečení zpracování

Hodnocení nastavení úrovně technických a organizačních opatření v jednotlivých oblastech fyzické, technické, personální (organizační) a administrativní bezpečnosti k eliminaci hrozby

Oblast	Popis hrozby	Hodnocení opatření	
1) Fyzická Zabezpečení budov	Průnik cizí neoprávněné osoby do objektu, kanceláří a místností s IT technikou většinou s cílem krádeže, případně poškození vybavení.	Celodenní dostatečné mechanické (mříže brány) a elektronické zabezpečení budov, vrátnice nebo kamera vstupu, čipový systém průchodu zaměstnanců, žáků, příp. ostraha, fyzická bezpečnost a pravidelnost záloh, DR plán.	**1**
		Celodenní dostatečné mechanické (mříže brány) a elektronické zabezpečení budov, vstupy do budov uzamčeny, cizí osoby průchod přes elektronické zámky na zvonky do kanceláří, existuje pravidelnost záloh.	**2**
		Některé vstupy do budov jsou částečně přístupné, vchody uzamčeny až po ukončení provozu, uplatněny mechanické zábrany, zálohy dat jsou různého data.	**3**
		Budovy jsou běžně přístupné, vchody uzamčeny až po ukončení provozu, žádné další personální, mechanické ani elektronické zabezpečení. V případě krádeže IT nejsou aktuální zálohy dat.	**4**
2) Fyzická Zabezpečení interiérů budov	Průnik další neoprávněné osoby (zaměstnanec, dítě, žák), do kanceláří a místností s IT technikou většinou s cílem krádeže (čtení, kopírování), případně poškození dat jak v listinné, tak elektronické podobě.	Nastaven a popsán klíčový režim, kanceláře uzamčeny, dokumenty s osobními údaji uzamčeny ve skříních, trezorech s mírou zabezpečení dle jejich klasifikace, PC v nepřítomnosti odhlášeny z profilu.	**1**
		Klíčový režim existuje částečně, kanceláře uzamčeny, dokumenty s osobními údaji uzamčeny ve skříních, PC v nepřítomnosti odhlášeny z profilu.	**2**
		Kanceláře uzamčeny, některé dokumenty s osobními údaji většinou uloženy v neuzamčených skříních. PC v nepřítomnosti bývají odhlášeny z profilu.	**3**
		Klíčový režim není uplatněn, kanceláře s osobními údaji jsou běžně přístupné včetně dokumentů s osobními údaji i po odchodu zodpovědné osoby, PC neodhlášeny z profilu.	**4**
3) Fyzická	Výpadek napětí, napěťové rázy a	UPS zdroje včetně ochrany el. anomálií implementovány na všech důležitých zařízeních pro	**1**

Oblast	Popis hrozby	Hodnocení opatření	
Napájení (elektrická energie)	další anomálie, hrozí poškození dat nebo jejich ztráta.	běh základního systému v případě krátkodobého výpadku. V případě poškození denní zálohy k dispozici, DR plán zpracován, zaměstnanci poučeni.	
		UPS zdroje nejsou na všech důležitých zařízeních pro běh systému, některé aplikace s daty jsou i pouze na lokálních PC bez UPS zdrojů. V případě poškození zálohy k dispozici.	**2**
		Nekontrolované zastaralé UPS bez požadované kapacity, zálohy jsou různého data.	**3**
		Žádná opatření nejsou uplatněna, zálohy dat nemusí být k dispozici.	**4**
4) Fyzická Živel	Voda: zaplavení prostor umístění serverů a PC s instalovanými hlavními informačními systémy s následným zničením dat. Spisovny a další místa uložení dat vedených v listinné podobě s hrozbou zničení. Oheň: zahoření prostor s následným zničením dat, žádné protipožární zabezpečení prostor umístění serverů a PC s informačními systémy. Spisovny a další místa uložení dat vedených v listinné podobě s hrozbou zničení.	Vhodné umístění serverové místnosti a její případná klimatizace, bezpečné umístění PC v kancelářích s instalovanými IS, vhodná samostatná místnost pro spisovnu, dostatečná protipožární opatření, fyzická bezpečnost všech záloh s osobními údaji je řešena (zálohy i na jiném místě, jiné budově apod.), DR plán.	**1**
		Vhodné umístění serverové místnosti, bezpečné umístění PC v kancelářích s instalovanými IS, vhodná samostatná místnost pro spisovnu, dostatečná protipožární opatření, není řešena fyzická bezpečnost veškerých záloh (zálohy i na jiném místě, jiné budově apod.), DR plán.	**2**
		Serverová místnost svými technickými parametry neodpovídá bezpečnému provozu nebo servery jsou různě po kancelářích, umístění PC v kancelářích s instalovanými IS není řešeno z hlediska bezpečného provozu.	**3**
		Žádná opatření proti hrozbě záplavy nebo požáru, v souvislosti s bezpečností dat nejsou učiněna.	**4**
5) Technická Kybernetický útok vnitřní	Virová nákaza, backdoor, trojský kůň, spyware, malware. Inicializace zevnitř organizace (např. doručeno jako příloha v e-mailu, staženo z webu	Antivirové programy jsou implementovány aktuální na všech úrovních, přihlašovací hesla mají definovanou strukturu. Školení zaměstnanců v oblasti počítačové bezpečnosti probíhá pravidelně. Operační systém je pravidelně aktualizován. Jsou implementovány všechny doporučené a kritické bezpečnostní záplaty. Je používána podporovaná verze OS. Jsou aktualizovány ovladače hardware a aktuální doporučená verze BIOS. Zálohy jsou	**1**

Oblast	Popis hrozby	Hodnocení opatření	
	nebo infiltrace z přenosného média). Zásadní roli zde hraje lidský faktor. Útočníci mohou získat dostatek údajů o struktuře sítě, hesla, firemní poštu. Vysoká hrozba katastrofického dopadu pro osobní údaje zejména ve smyslu jejich zničení.	dostupné, aktuálního data ze všech zařízení. Oddělená fyzická bezpečnost záloh existuje. Je zpracován krizový plán a scénáře pro minimalizaci škod, DR plán.	
		Antivirové programy jsou implementovány aktuální na všech úrovních, přihlašovací hesla mají definovanou strukturu. Školení zaměstnanců v oblasti počítačové bezpečnosti probíhá pravidelně. Zálohy jsou dostupné, aktuálního data ze všech zařízení. Oddělená fyzická bezpečnost záloh neexistuje.	**2**
		Antivirové programy jsou implementovány ale jejich nastavení a aktuálnosti na všech úrovních není věnována dostatečná pozornost, přihlašovací hesla nemají definovanou strukturu (slabá). Někteří zaměstnanci neřeší možné nebezpečí hrozící z Internetu, emailu, školení zaměstnanců neprobíhá. Zálohy jsou dostupné, různého data.	**3**
		Antivirovým programům a jejich nastavení a aktuálnosti není věnována pozornost, není instalován na všech zařízeních, přihlašovací hesla jsou používána sporadicky, zaměstnanci nemají povědomí o hrozbách z emailu, Internetu, nebo infiltrací z přenosných médií. Zálohy nejsou nebo jen lokální a sporadické.	**4**
6) Technická Kybernetický útok vnější	Zahájen z vnějšku bezpečnostního obvodu, neoprávněnou osobou nebo neoprávněným uživatelem systému. (Skenování portů, DDoS IP spoofing). Hrozí nebezpečí nedostupnosti služby, neoprávněného přístupu s plným nebo částečný přístupem k zařízení včetně neautorizovaných	Routery a firewally jsou správně nastaveny, je prováděn monitoring síťového provozu s logováním, je prováděno vyhodnocování incidentů a realizována opatření. Silnou stránkou zabezpečení síťového provozu jsou demilitarizované zóny, segmentace sítě, nastavení firewallu, řízení podle MAC adres, strukturovaná síla hesel. Oprávnění přístupů definována v celé struktuře podle rolí. Oddělená fyzická bezpečnost záloh existuje. Je zpracován krizový plán a scénáře pro minimalizaci škod, DR plán.	**1**
		Routery a firewally jsou správně nastaveny, je prováděn monitoring síťového provozu, je prováděno vyhodnocování incidentů a realizována opatření. Silnou stránkou zabezpečení síťového provozu je nastavení firewallu, strukturovaná síla hesel. Oprávnění přístupů definována v celé struktuře podle rolí. Oddělená fyzická bezpečnost záloh neexistuje.	**2**

Oblast	Popis hrozby	Hodnocení opatření	
	změn v konfiguraci, mazání nebo modifikaci souborů s výsledkem získání informací.	Routery a firewally jsou správně nastaveny. Síťový provoz je monitorován pouze v případě výpadku. Ne všechna zařízení v síti jsou podřízena oprávnění přístupů podle rolí. Síla a struktura hesel není uplatňována, Oddělená fyzická bezpečnost záloh neexistuje.	**3**
		Provoz sítí a služeb byl na počátku nastaven (např. externím dodavatelem) a není již nadále monitorován a pravidelně aktualizován. Zálohy nejsou nebo jen lokální a sporadické. Provoz sítí vykazuje výpadky, narušení byla v minulosti detekována	**4**
7) Technická Hardware, software	Zastaralý hardware, nebezpečí ztráty dat při selhání, problematické řešení bezpečnostních problémů. Software a jeho provoz po ukončení podpory výrobce (WIN XP, Office 2003 a další aplikace pro práci s OÚ).	Organizace se řídí plánem obnovy a údržby hardware a software. Všechna zařízení jsou pravidelně aktualizována. Nepoužívá se software, ke kterému již není poskytovaná podpora výrobcem.	**1**
		Organizace se řídí plánem obnovy a údržby hardware a software. Všechna zařízení jsou pravidelně aktualizována. Na některých stanicích se vyskytuje software bez podpory poskytované výrobcem.	**2**
		Data jsou v některých případech zpracovávána na prostředcích hraničící s jejich životností. Na software bez podpory výrobcem není brán zřetel	**3**
		Na stáří hardware a software není brán zřetel, k výměně dochází zejména po selhání.	**4**
8) Lidské zdroje Činnost administrátorů	Nedostatečné, nevhodné nebo nahodilé rozdělení rolí mezi administrátory. Nejasné role mezi interními a externími administrátory při správě sítí externími firmami při outsourcingu.	Role administrátorů sítí jsou jednoznačně stanoveny ve vnitřních předpisech, oprávnění jsou řešena podle rolí, administrátorské účty na lokálních PC jsou omezeny na minimum. S externím správcem sítí jsou uzavřeny dodatky smluv se stanovenými povinnostmi v souladu s ustanoveními o ochraně osobních údajů. Jsou definovány závazky mlčenlivosti atd., vedeny administrátorské deníky.	**1**
		Role administrátorů sítí jsou stanoveny, oprávnění jsou řešena podle rolí, administrátorské účty na lokálních PC se vyskytují. S externím správcem sítí jsou uzavřeny dodatky smluv se stanovenými povinnostmi v souladu s ustanoveními o ochraně osobních údajů.	**2**
		Role administrátorů sítí nejsou stanoveny, s externím správcem sítí není uzavřena smlouva s dodatky v souladu s GDPR, účty na lokálních PC jsou většinou s plnými přístupy.	**3**
		Oficiální administrátor neexistuje, na správě sítí se podílí další osoby bez stanovených oprávnění.	**4**

Oblast	Popis hrozby	Hodnocení opatření	
9) Lidské zdroje Personální bezpečnost	Zaměstnanci bez patřičných kvalifikačních předpokladů pro výkon funkcí s přímým zpracováním osobních údajů (zejména sekretářky, personalisté, mzdové účetní apod.) nebo zaměstnanci zajišťující správu informačních systémů a aplikací (administrátoři, technici, opraváři) a další osoby spolupracujících třetích stran.	Zaměstnanci jsou na všech úrovních odborně kvalifikováni. Bezpečnostní povědomí je na vysoké úrovni, pravidelně se účastní školení jak oborového, tak bezpečnostního. Dokážou použít zpracované návody postupů při bezpečnostních incidentech. Na potřebných pozicích jsou upraveny pracovní smlouvy ve vztahu k mlčenlivosti apod., náplně práce jsou aktuální.	**1**
		Zaměstnanci jsou většinou odborně kvalifikováni. Pravidelně se účastní školení jak oborového, tak bezpečnostního. Jsou seznámeni s postupy při bezpečnostních incidentech. Na potřebných pozicích jsou upraveny pracovní smlouvy ve vztahu k mlčenlivosti apod., náplně práce jsou aktuální.	**2**
		Zaměstnanci většinou nejsou odborně kvalifikováni. Školení jak oborového, tak bezpečnostního se účastní nepravidelně. Jsou seznámeni s postupy při bezpečnostních incidentech.	**3**
		S osobními údaji pracují zaměstnanci bez odborné kvalifikace, zaměstnanci se neúčastní školení k bezpečnostnímu povědomí při zpracovávání osobních údajů, administrátoři nemají žádnou kvalifikaci ke správě sítí.	**4**
10) Lidské zdroje Řízení přístupů k IS	Žádné nebo nedostatečné vymezení funkcí a rolí v IS, nedefinovaná přístupová práva zaměstnanců u uživatelských účtů, opomíjený životní cyklus účtů, široce nastavené přístupy k síťovým službám, aplikacím, zálohám, terminálům, emailovým účtům nezavedena správa a determinace tvorby hesel.	Komplexně zpracovaná a popsaná politika řízení přístupů v organizačních směrnicích organizace s vymezením rolí a diferencovaných přístupů jak v operačních systémech jednotlivých PC, tak v aplikacích pro práci s osobními údaji. Popsán a důsledně uplatňován životní cyklus přístupů k uživatelským účtům a emailům. Jsou nastavena pravidla pro kvalitu a sílu hesel.	**1**
		Politika řízení přístupů je roztříštěna v různých organizačních směrnicích. Role a přístupy do operačních systémů jednotlivých PC i aplikací pro práci s osobními údaji jsou většinou popsány. Životní cyklus přístupů k uživatelským účtům a emailům není v předpisech stanoven. Jsou nastavena pravidla pro kvalitu a sílu hesel.	**2**
		Politika řízení přístupů a rolí není popsána, přístupy jsou jen nastaveny administrátorem systému. Není popsán a důsledně uplatňován životní cyklus přístupů k uživatelským účtům a emailům. Nejsou nastavena pravidla pro kvalitu a sílu hesel.	**3**
		Nejsou nastavena žádná pravidla.	**4**

Oblast	Popis hrozby	Hodnocení opatření	
11) Lidské zdroje Management bezpečnosti lidských zdrojů	Neškolení zaměstnanci bez informací o hrozbách plynoucích z používání Internetu, neznámých webových stránek, emailové pošty. Nepoučení zaměstnanci o sociálním inženýrství (Phising, Pretexting, Baiting apd.). Neoprávněná instalace software. Neznalost postupů v případě incidentu.	Zaměstnanci jsou pravidelně školení v otázkách bezpečnosti v používání Internetu, emailové pošty, znají své role a povinnosti uživatelů při instalaci software, jsou obeznámeni s postupy v případech incidentů včetně jejich hlášení. Jsou obeznámeni s užitím technologií při výuce, a to i ve vztahu k používání technologií žáky. Jsou obeznámeni s příčinami i důsledky bezpečnostních incidentů, pokud se vyskytly.	**1**
		Zaměstnanci jsou školení v otázkách bezpečnosti v používání Internetu, emailové pošty, znají své role a povinnosti uživatelů při instalaci software, jsou obeznámeni s postupy v případech incidentů včetně jejich hlášení. Jsou obeznámeni s užitím technologií při výuce, a to i ve vztahu k používání technologií žáky.	**2**
		Zaměstnanci nejsou pravidelně školení v otázkách bezpečnosti v používání Internetu, emailové pošty, neznají své role a povinnosti uživatelů při instalaci software. Mají povědomí o bezpečném užití technologií při výuce, a to i ve vztahu k používání technologií žáky.	**3**
		Zaměstnanci se neúčastní žádného školení bezpečnosti, neznají své role a povinnosti uživatelů při instalaci software, nejsou obeznámeni s postupy v případech incidentů. Mají pouze částeční povědomí o bezpečném užití technologií při výuce, a to i ve vztahu k používání technologií žáky.	**4**
12) Lidské zdroje Lidské zdroje, monitoring a kontrola	Nezajištěná preventivní kontrola dodržování bezpečnostní politiky vyplývající z organizačních směrnic organizace z pozice hierarchie jednotlivých rolí a postavení zaměstnanců (hlavní administrátor x administrátoři x uživatelé, statutární orgán x vedení organizace x zaměstnanci).	Organizace má směrnicí stanovena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. Přístupy jsou pravidelně přezkoumávány jak k serverům, tak i ke koncovým zařízením. Síťové logy jsou pravidelně kontrolovány.	**1**
		Organizace má směrnicí stanovena pravidla a postupy pro řešení některých případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. Přístupy ani síťové logy nejsou pravidelně přezkoumávány a kontrolovány.	**2**
		Organizace nemá směrnicí stanovena pravidla a postupy pro řešení některých případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. Přístupy ani síťové logy nejsou kontrolovány.	**3**
		Organizace nemá stanovena žádná pravidla k dodržování bezpečnostních pravidel.	**4**

Oblast	Popis hrozby	Hodnocení opatření	
13) Administrativní Spisový, skartační a archivní řád	Zastaralá dokumentace neodpovídající skutečnosti, chybějící definice oběhu písemností, nedefinované nebo nesprávně stanovené skartační lhůty, chybějící směrnice pro manipulaci s nosiči informací v elektronické podobě (datové schránky, el. spisové služby, konverze apod.). Osobní údaje jsou uchovávány i po expiraci doby pro skartaci.	Organizace má platný spisový a skartační řád s platnými lhůtami pro skartaci a archivaci dokumentů s osobními údaji. Oběh dokumentů v organizace je dodržován v souladu se spisovým řádem, jsou stanoveny odpovědnosti na jednotlivých úsecích zpracování. Zaměstnanci při oběhu dokumentů v elektronické podobě postupují podle stanovených postupů ve spisovém řádu a dalších směrnicích. Jsou stanovena pravidla pro přenos dokumentů, a to jak elektronických, tak v listinné podobě.	**1**
		Organizace má platný spisový a skartační řád s platnými lhůtami pro skartaci a archivaci dokumentů s osobními údaji. Oběh dokumentů v organizaci ne vždy postupuje dle stanovených pravidel a v souladu se spisovým řádem. Odpovědnostní role za zpracování na jednotlivých úsecích nejsou stanoveny. Zaměstnanci mají obecně stanovena pravidla pro oběh dokumentů v elektronické podobě. Pravidla pro přenos dokumentů, a to jak elektronických, tak v listinné podobě jsou stanovena pouze obecně.	**2**
		Organizace má spisový a skartační řád, platnost lhůt pro skartaci a archivaci dokumentů s osobními údaji není ověřena. Pro oběh dokumentů v organizaci nejsou stanovena pravidla. Odpovědnostní role za zpracování na jednotlivých úsecích nejsou stanoveny. Zaměstnanci nemají pro oběh a přenos dokumentů v listinné a elektronické stanovena žádná pravidla.	**3**
		Organizace nezavedla spisový a skartační řád.	**4**
14) Administrativní Směrice	Zastaralé směrnice, vnitřní předpisy, pokyny apod. neodpovídající zákonu č. 101/2000 Sb., o ochraně osobních údajů a Nařízení Evropského parlamentu a Rady (EU) 2016/679. Chybějící role pro práci s osobními údaji. Nestanovená odpovědnost za	Organizace má aktualizovanou základní směrnici (předpis, pokyn apod.), k ochraně osobních údajů, která je v souladu s ustanoveními zákona č. 101/2000 Sb., o ochraně osobních údajů a je doplněna o ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679. Všechny ostatní navazující předpisy v organizaci (např. organizační řád, platový předpis, směrnice k zabezpečení IS apod.), které se ve svých ustanoveních dotýkají ochrany osobních údajů jsou rovněž aktualizovány a jsou v souladu se základní směrnicí.	**1**
		Organizace má aktualizovanou základní směrnici (předpis, pokyn apod.), k ochraně osobních údajů, která je v souladu s ustanoveními zákona č. 101/2000 Sb., o ochraně osobních údajů a je doplněna o ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679. Ne všechny ostatní navazující předpisy v organizaci (např. organizační řád, platový předpis, směrnice	**2**

Oblast	Popis hrozby	Hodnocení opatření	
	jednotlivá zpracování.	k zabezpečení IS apod.), které se ve svých ustanoveních dotýkají ochrany osobních údajů jsou rovněž aktualizovány a jsou v souladu se základní směrnicí.	
		Organizace má základní směrnici (předpis, pokyn apod.), k ochraně osobních údajů, která je v souladu s ustanoveními zákona č. 101/2000 Sb., o ochraně osobních údajů. Vazby na ostatní vnitřní předpisy nejsou, neodpovídají současné legislativě.	**3**
		Organizace nemá aktuální směrnici k ochraně osobních údajů, v ostatních směrnicích školy se tématika ochrany osobních údajů vyskytuje pouze sporadicky.	**4**

1.3. Hodnocení rizik s dopadem do GDPR

Při posuzování úrovně bezpečnosti se zde hodnotí zejména rizika, která představuje zpracování, jako náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům.

GDPR - Rizika	**Náhodné nebo protiprávní zničení osobních údajů** Míra rizika je průnikem fyzické a kybernetické bezpečnosti, působením lidských zdrojů a rizik z administrativní oblasti.	1,00 až 2,00	**nízké**
		2,01 až 2,50	**střední**
		2,51 až 3,00	**vysoké**
		3,00 až 4,00	**kritické**
	Ztráta osobních údajů Míra rizika je průnikem fyzické a kybernetické bezpečnosti, působením lidských zdrojů a rizik z administrativní oblasti.	1,00 až 2,00	**nízké**
		2,01 až 2,50	**střední**
		2,51 až 3,00	**vysoké**
		3,00 až 4,00	**kritické**
	Pozměňování osobních údajů Míra rizika je průnikem fyzické a kybernetické bezpečnosti, působením lidských zdrojů a rizik z administrativní oblasti.	1,00 až 2,00	**nízké**
		2,01 až 2,50	**střední**
		2,51 až 3,00	**vysoké**
		3,00 až 4,00	**kritické**
	Neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů Míra rizika je průnikem fyzické a kybernetické bezpečnosti, působením lidských zdrojů a rizik z administrativní oblasti.	1,00 až 2,00	**nízké**
		2,01 až 2,50	**střední**
		2,51 až 3,00	**vysoké**
		3,00 až 4,00	**kritické**

1.4. Kalkulačka rizik

Kalkulačka rizik je nástroj pro hodnocení a výpočet míry rizika jednotlivých zpracování. Kalkulačka je přílohou tohoto dokumentu v listu EXCEL a je otevřena k posuzování rizik zpracování jak současných, zjištěných v rámci této analýzy, tak případných nových zpracování.

Rizika jsou hodnocena

- celkem za jednotlivá zpracování
- jednotlivě z hlediska náhodného nebo protiprávního zničení, ztráty, pozměňování, neoprávněného zpřístupnění zpracovávaných osobních údajů
- jednotlivá zpracování ke konkrétní oblasti bezpečnosti fyzické, technické, personální (organizační) a administrativní

Hodnotící stupnice rizika

- nízké
- střední
- vysoké
- kritické

Výpočtové vzorce a algoritmy hodnocení včetně nápovědy k jednotlivým zpracováním jsou součástí uvedené kalkulačky v listu Excel.

Část I: Vzor evidenčního listu souhlasů subjektů údajů

Evidenční list souhlasů subjektů údajů č….			**Dle čl. 6 odst. 1. písm. a) GDPR**			**List 1/..**
Subjekt osobních údajů	Výčet osobních údajů, ke kterým byl udělen souhlas	Konkrétní účel zpracování, ke kterému byl souhlas udělen	Předání	Datum udělení souhlasu	Datum nebo lhůta pro výmaz	Pozn.

Část J: Závěrečná ustanovení

1. Tato směrnice nabývá účinnosti dne 25. května 2018 a vydává se na dobu neurčitou.

V Opavě dne 25. května 2018

…….……

Ing. Vítězslav Doleží, v. r.

ředitel školy,

Střední škola průmyslová a umělecká,

Opava, příspěvková organizace

Příloha č. 5 Směrnice

Personální organizační opatření k zajištění ochrany osobních údajů

Přijatá organizační opatření dle části G článku II, odst. 1. písm. c. Zásad zpracování osobních údajů

Příloha č. 2 Směrnice

odst. 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.

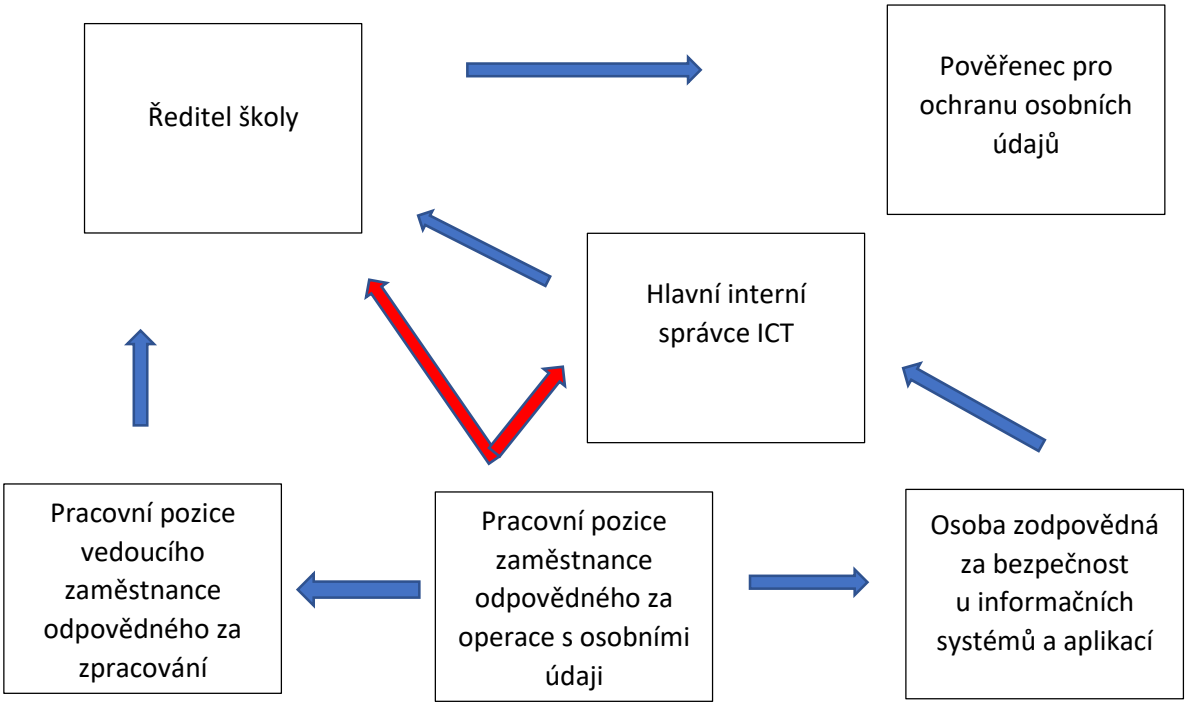
odst.) 4

- Ihned po zjištění, nejpozději do 48 hodin, možného bezpečnostního incidentu ředitel kontaktuje pověřence, se kterým zkonzultuje další postup

Struktura hlášení bezpečnostních incidentů (narušení zabezpečení osobních údajů)

Základní princip toku informací

a) je povinností každého zaměstnance ihned po zjištění možného bezpečnostního incidentu informovat svého nadřízeného zaměstnance o události
b) níže uvedený princip toku informací se přiměřeně použije dle reálné situace a intenzity hrozby



Organizační struktura			
Ředitel školy		**Pověřenec pro ochranu osobních údajů**	
	Hlavní interní správce ICT		
	Odpovědné osoby za hlavní účely zpracování osobních údajů		
Zpracování	Pracovní pozice vedoucího zaměstnance odpovědného za uvedené zpracování	Pracovní pozice zaměstnanců odpovědných za operace s osobními údaji	Osoba zodpovědná za bezpečnost zpracování u informačních systémů a aplikací
Přijímání ke vzdělávání	Ředitel školy	ZŘŠ + sekretářka	ICT správce ICT koordinátor
Průběh vzdělávání	Ředitel školy	ZŘŠ + sekretářka	
Ukončování vzdělávání	Ředitel školy	ZŘŠ + sekretářka	
Zajištění odborné praxe	Ředitel školy	Učitel odborných předmětů	
Školní matrika	Ředitel školy	ZŘŠ + sekretářka, výchovný poradce	
Poskytování služeb ŠPP	Ředitel školy	Výchovný poradce, školní metodik prevence	
Jazykové vzdělávání	Ředitel školy	Předseda předmětové komise cizích jazyků	
Erasmus+	Ředitel školy	Manažer projektu, finanční manažer projektu	
Rozhodování ve správním řízení	Ředitel školy	ZŘŠ	
Organizace exkurzí a sport. akcí	Ředitel školy	Pedagog – vedoucí akce	
Prezentace školy, web, média	Ředitel školy	ICT koordinátor	
Výběrová řízení do zaměstnání	Ředitel školy	ZŘŠ	
Pracovní a mzdová agenda	Ředitel školy	Sekretářka, ekonomka	
Vzdělávání zaměstnanců a DVPP	Ředitel školy	Pedagog – organizátor DVPP	
Evidence pracovní doby	Ředitel školy	ZŘŠ, vedoucí úseku správních zaměstnanců	
Bezpečnost – kamerové systémy	Ředitel školy	Správce budov	
BOZ a BOZP, události a úrazy	Ředitel školy	Osoba pověřená péčí o BOZP, sekretářka	
Vedení účetnictví	Ředitel školy	ekonomka	
Smluvní vztahy a DPČ	Ředitel školy	Referentka majetkové správy, sekretářka	
Projekty, žádosti o dotace	Ředitel školy	Finanční manažer, ekonomka	
Školní knihovna	Ředitel školy	Pedagog	

V Opavě dne 25. 5. 2018

Podpis ředitele školy: Ing. Vítězslav Doleží, v. r.