VNITŘNÍ PŘEDPIS O ZPRACOVÁNÍ A OCHRANĚ OSOBNÍCH ÚDAJŮ

platný a účinný od 01. 09. 2024

Základní umělecká škola Police nad Metují, okres Náchod
se sídlem: *Komenského nám. 108, 549 54 Police nad Metují*
IČO: *62728814*
právní forma: *příspěvková organizace*
zřizovaná: *Město Police nad Metují*
zastoupená: *Alžbětou Černou (ředitelkou školy)*
kontaktní údaje: e-mail: *zus@zuspolice.cz*
telefon: *+420 605 905 420*
(dále také „zaměstnavatel“)

vydává podle **§ 305 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů (dále jen „zákoník práce“)** tento

VNITŘNÍ PŘEDPIS

kterým se blíže upravují práva a povinnosti zaměstnanců upravené v 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, v platném znění (dále jen „Nařízení“) a podle zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů**, jakož i vnitřní organizace zaměstnavatele při zpracování a ochraně osobních údajů**

I. PŮSOBNOST

Tento vnitřní předpis stanovuje práva a povinnosti zaměstnanců při zpracování osobních údajů, a to jak při ručním, tak při automatizovaném zpracování. Vztahuje se na všechny zaměstnance organizace a upravuje komplexně oblast ochrany osobních údajů.

II. DEFINICE A POJMY

Pro účely tohoto vnitřního předpisu se rozumí:

a) Nařízením 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).

b) Osobním údajem (dále také jako „OÚ“) každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat.

c) Citlivými osobními údaji (tzv. zvláštní kategorie osobních údajů) údaje, které mohou subjekt údajů samy o sobě poškodit (např. ve společnosti, zaměstnání, škole) či mohou zapříčinit jeho diskriminaci. Jde zejména o: *národnostní, rasový nebo etnický původ, politické postoje, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofické přesvědčení, údaje o trestné činnosti, zdravotní stav a sexuální život*.

d) Subjektem údajů fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

e) Správcem osobních údajů (dále také „Správce“) Zaměstnavatel. Správci osobních údajů sami nebo společně určují účely (na základě čeho) a prostředky zpracování (formu)

f) Zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který na základě zákona nebo pověření Správce zpracovává osobní údaje pro správce

g) Příjemcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce

nepovažují (inspekční a vyšetřovací orgány jako PČR, FÚ, ČOI, ÚOHS aj.). Zpracování osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

h) Zpracováním osobních údajů jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Zpracování osobních údajů je nutné považovat za sofistikovanější činnost, kterou správce osobních údajů nebo zpracovatel s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky.

i) Profilováním jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

j) Pseudonymizací zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

k) Anonymizací Zpracování osobních údajů způsobem, že nemohou být již nikdy přiřazeny konkrétnímu subjektu a jeho identifikaci ani nenapomáhají.

l) Souhlasem subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Může být učiněn písemně, elektronicky i ústně.

m) Pověřencem pro ochranu osobních údajů (dále také „DPO“ nebo „pověřenec“) pozice v rámci organizace, v níž působí zaměstnanec nebo externí pracovník jako ochránce osobních údajů zaměstnanců, občanů, klientů, zákazníků, dodavatelů a dalších fyzických osob, jejichž údaje Správce osobních údajů zpracovává. Funguje mj. jako prostředník pro komunikaci mezi subjektem údajů, správcem a dozorovým úřadem.

n) Odpovědnou osobou osoba uvedená v čl. IV. tohoto vnitřního předpisu.

o) Bezpečnostním incidentem porušení zabezpečení / únik dat – náhodné nebo protiprávní zničení, ztráta, změna nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních dat.

p) Kategoriemi OÚ: adresní, identifikační, zvláštní a popisné.

   Adresní (kontaktní) a identifikační údaje jsou údaje k jednoznačné a nezaměnitelné identifikaci a umožňující kontakt se subjektem údajů (např. jméno, příjmení, titul, rodné číslo, datum narození, adresa trvalého pobytu, kontaktní nebo doručovací adresa, místo narození, státní příslušnost, pohlaví, u fyzické osoby podnikající též daňové identifikační číslo a IČ, dále kontaktní adresa, číslo telefonu, e-mailová adresa, jméno datové schránky).

   Popisné údaje jsou údaje vytvářející komplexní obraz fyzické osoby (například údaje o vzdělání, znalosti cizích jazyků, odborné znalosti a dovednostech, počtu dětí, informace o absolvování vojenské služby, o předchozím zaměstnání, zdravotní pojišťovně, mzdě, ale také vzhled, výška, postava, barva vlasů apod.)

   Zvláštní – viz. odstavec II., písm. c)

q) Úřadem je Úřad pro ochranu osobních údajů České republiky (dále také ÚOOÚ).

r) Zaměstnancem se pro účely tohoto vnitřního předpisu rozumí i statutární orgán, pokud je dle čl. IV. odpovědný za plnění povinností dle tohoto vnitřního předpisu.

III. KATEGORIE OSOBNÍCH ÚDAJŮ, ÚČELY A PRÁVNÍ TITULY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. Zaměstnavatel zpracovává tyto kategorie OÚ:
   a) Adresní, identifikační a popisné

b) Zvláštní, zejména údaje o zdravotním stavu, údaje o trestné činnosti, zdravotní stav, biometrické údaje (sloužící k identifikaci fyzické osoby) a členství v odborové organizaci, je-li zřízena

2. Zaměstnavatel zpracovává OÚ za účelem plnění pracovněprávních povinností, za účelem plnění smluvních povinností se svými obchodními partnery a pro účely plnění povinností uložených mu platnými zákony.

3. Právním titulem pro zpracování osobních údajů u zaměstnavatele je především plnění zákonných povinností, plnění smlouvy, oprávněný zájem, veřejný zájem a v odůvodněných případech souhlas se zpracováním osobních údajů nebo ochrana životně důležitých zájmů subjektu údajů.

IV. ODPOVĚDNÉ OSOBY

1. Osobou odpovědnou za dodržování povinností podle Nařízení a souvisejících právních předpisů je u zaměstnavatele: *ředitelka školy – statutární zástupce*,

2. Osobou pověřenou implementací a kontrolou bezpečnostních a technicko-organizačních opatření v souvislosti se zpracováním a ochranou OÚ (dále také „Pověřená osoba“) je: *ředitelka školy – statutární zástupce*,

3. Pro účely kontaktování Pověřené osoby v případech dotazů, námitek a žádostí souvisejících s bezpečností, ochranou a zpracováním osobních údajů a hlášení bezpečnostních událostí a incidentů se stanovují tyto kontaktní údaje:
e-mailová adresa: *cerna.alzbeta@zuspolice.cz*.

   Za vyřízení zákonných žádostí a námitek došlých na uvedený e-mail je odpovědná: *Pověřená osoba*.

4. V ostatních případech je za dodržení povinností uvedených v tomto předpisu odpovědný zaměstnanec, který OÚ zpracovává a kterého zaměstnavatel pověřil úkoly spojenými s ochranou OÚ v rámci jeho organizační struktury. Zpracováním osobních údajů jsou pak zejména pověřeni zaměstnanci účetního a personálního oddělení.

5. Pověřencem pro ochranu osobních údajů je jmenována: *Ing. Mgr. Petra Pavelková*
Kontaktní e-mail: *poverenec@zuspolice.cz*
Kontaktní telefonní číslo: *+420 777 072 276*

V. PRÁVA A POVINNOSTI

Povinnosti zaměstnanců

1. Všichni zaměstnanci jsou povinni při výkonu práce zajistit, aby nebyly OÚ zpřístupněny neoprávněným příjemcům a dodržovat mlčenlivost o OÚ všech subjektů údajů, se kterými přijde při výkonu práce do styku. Zaměstnanec zpracovává OÚ subjektů údajů pouze na pokyn zaměstnavatele zákonně, korektně, transparentně, k účelu, ke kterému byly údaje subjektem údajů poskytnuty, v minimálním nezbytném rozsahu, přesně, po dobu ne delší, než je nezbytné pro účel zpracování, a způsobem, který zajistí náležité zabezpečení OÚ včetně jejich ochrany.

2. Zaměstnanec musí dodržovat mlčenlivost o svých přístupových údajích a heslech do počítačových systémů zaměstnavatele. Zaměstnanec je povinen listinné nosiče OÚ (dokumenty) v době, kdy s nimi nepracuje, odpovídajícím způsobem zabezpečit před neoprávněným přístupem, poškozením, zneužitím či ztrátou. Zaměstnanec je povinen se odhlásit z počítačového systému nebo uzamknout prostředí operačního systému při vzdálení se od počítače zaměstnavatele, na kterém pracuje, a zabezpečit svěřenou techniku před neoprávněným přístupem.

3. Jsou-li zpracovávány OÚ na základě souhlasu subjektu údajů, musí být souhlas písemný a musí být uložen v listinné nebo elektronické podobě ve spisovně nebo elektronické složce na serveru ZUŠ, aby byl doložitelný. Zaměstnanec, který souhlas připravuje, je povinen jako výchozí vzor použít souhlas, který mu na žádost poskytne Pověřená osoba a vždy informovat subjekt údajů, že souhlas je odvolatelný zasláním žádosti na oficiální e-mailovou adresu školy, pověřené osoby, poštovní adresu zaměstnavatele.

4. Zpracovává-li zaměstnanec OÚ subjektu údajů mladšího 18 let v případech, kdy není zpracování stanoveno právní povinností nebo ochranou životně důležitých zájmů subjektu údajů, je povinen tak činit se souhlasem a schválením zákonného zástupce (rodiče subjektu údajů, soudem učený poručník nebo osvojitel). Zaměstnanec vyvine přiměřené úsilí, aby ověřil, že souhlas byl dán opravdu zákonným zástupcem.

5. Zakazuje se zpracování OÚ, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby, nejde-li o zákonem stanovené výjimky spočívající ve vedení personálních agend nebo plnění úkolů nezbytných pro splnění úkolů daných platnými zákony.

Práva subjektu údajů

1. Získává-li zaměstnanec OÚ od subjektu údajů, splní vůči subjektu údajů informační povinnost o jeho právech a poskytne potřebná sdělení minimálně v rozsahu aktuálně platného dokumentu *„Zásady zpracování osobních údajů a informace o pořizování fotografií a audio-video záznamů*“, umístěného v listinné podobě v kanceláři školy a v elektronické podobě na oficiálních stránkách školy (*https://zuspolice.cz/; sekce „Dokumenty školy“ \ „Ochrana osobních údajů“*) kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

2. Zaměstnanec, který je zaměstnavatelem pověřen komunikací se subjekty údajů v případech, kdy realizují svoje práva, poskytne subjektu údajů na žádost o přístup, žádost o informaci, zda a jaké OÚ se zpracovávají, opravu, výmaz, omezení zpracování, přenositelnost OÚ nebo vznese-li námitku či požádá-li o zrušení automatizovaného zpracovávání či profilování informace o přijatých opatřeních do jednoho měsíce od obdržení žádosti, jinak informuje subjekt údajů bezodkladně, nejpozději do 1 měsíce, o důvodech nepřijetí opatření a o možnosti podat stížnost u Úřadu pro ochranu osobních údajů.

3. Nezískává-li zaměstnanec OÚ od subjektu údajů, splní vůči subjektu údajů informační povinnost minimálně odkazem na aktuálně platný dokument *„Zásady zpracování osobních údajů a informace o pořizování fotografií a audio-video záznamů*“, umístěný v listinné podobě v kanceláři školy a v elektronické podobě na oficiálních stránkách školy (*https://zuspolice.cz/; sekce „Dokumenty školy“ \ „Ochrana osobních údajů“*), kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

4. Zaměstnanec vymaže OÚ, jestliže:
   a) OÚ již nejsou potřebné,
   b) jestliže subjekt údajů odvolá souhlas a neexistuje žádný další důvod pro zpracování,
   c) subjekt údajů vznese oprávněnou námitku proti zpracovávání OÚ na základě oprávněného zájmu Správce nebo proti automatizovanému individuálnímu rozhodování nebo proti profilování,

d) jestliže OÚ byly zpracovávány protiprávně,
e) jestliže OÚ musí být vymazány ke splnění právní povinnosti,
kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

Jestliže má být OÚ vymazán, zaměstnanec informuje zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby je vymazali.

5. Zaměstnanec je povinen předem upozornit subjekt údajů, kterému bylo omezeno zpracování OÚ, že omezení bude zrušeno.

6. Zaměstnanec je povinen oznámit veškerým příjemcům, jimž byly OÚ zpřístupněny, veškeré opravy, výmazy, omezení s výjimkou toho, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Zaměstnanec informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje, kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

7. Zaměstnanec vyřizuje námitky subjektu údajů proti zpracování OÚ, které se ho týkají, a byly získány ke splnění úkolu ve veřejném zájmu nebo na základě oprávněného zájmu Zaměstnavatele, včetně profilování, námitky proti zpracování OÚ pro přímý marketing, které se ho týkají, což zahrnuje i profilování.

VI. TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

1. Zaměstnavatel provádí následující opatření:

a) Vstupní analýza zpracování OÚ – Před účinností tohoto vnitřního předpisu a ke správnému nastavení opatření provedl zaměstnavatel analýzu současného stavu zpracovávání osobních údajů.
b) Kybernetická bezpečnost – Zaměstnavatel zpracovává OÚ v elektronické podobě pomocí informačních systémů a webových aplikací, které fungují typicky v prostředí Linux, Apple MAC OS, Apple IOS, Google Android a Microsoft Windows. Uživatelem jsou jen zaměstnanci, kteří se do prostředí a informačních systémů přihlašují uživatelským jménem a heslem. OÚ představující vysoké riziko zaměstnavatel šifruje, pseudonymizuje nebo chrání dalšími technickými opatřeními odpovídajícími míře rizika zpracovávaných údajů. Pro zpracování OÚ jsou využívány zejména tyto aplikace: informační systém iZUŠ, AVENSIO, e-Obec a další aplikace v rámci využívání operačního systému Microsoft Windows a kancelářského balíku Microsoft Office.
c) OÚ v elektronické podobě jsou ukládány na zabezpečených úložištích spravovaných školou a firmou Sensio.cz s.r.o. Zabezpečení je realizováno formou aktualizovaného antivirového programu, dalšími bezpečnostními opatřeními, případně bezpečnostními politikami, jakož i firewallem a dalšími obrannými systémy serveru a ochranou počítačové sítě proti útokům z internetu. Současně je prováděno zálohování dat na síťové diskové úložiště (NAS) a bezpečná cloudová úložiště provozovaná důvěryhodnými poskytovateli.

   Zaměstnanec musí při ukládání a zálohování dat dbát pokynů IT pracovníka a/nebo Pověřené osoby, nesmí provádět ukládání a zálohování na neschválená a neevidovaná zařízení (např. externí pevné disky, flashdisky, DVD/CD média). Bez schválení statutárního zástupce nesmí zaměstnanec připojit ke svěřené výpočetní technice soukromé periferní zařízení nebo zařízení pro ukládání dat (externí pevné disky, flashdisky). Zálohování na soukromá zařízení je přísně zakázáno!

   Zaměstnanec musí konzultací s IT pracovníkem zajistit zálohování svých dat ukládáním na předem určená síťová úložiště a umístění, případně cloudové systémy. Bez předchozího schválení IT pracovníka či Pověřené osoby není povoleno ukládat data přímo v lokálních aplikacích nebo složkách v osobních počítačích.

d) Elektronická komunikace probíhá prostřednictvím zabezpečeného e-mailového serveru, datové schránky, a v nutných případech se zaručeným elektronickým podpisem, kterým zaměstnavatel a vybraní zaměstnanci disponují.
e) Analýza rizik – Zaměstnavatel provedl analýzu relevantních rizik v oblasti ochrany a zpracování OÚ.
f) Fyzická bezpečnost – Zaměstnavatel zpracovává OÚ v listinné podobě na nosičích OÚ. Zaměstnanci dodržují ochranu OÚ tak, že minimalizují množství OÚ, které zpracovávají, listinné nosiče OÚ zamykají do stolních zásuvek, spisoven, skříní apod. a kanceláře a vstup do prostor využívaných pro ukládání a zpracovávání osobních údajů chrání elektronickým zabezpečovacím systémem a kamerovým systémem. Bez předchozího schválení statutárního zástupce/vedoucího pracovníka není dovoleno vynášet listinnou podobu dokumentů obsahující osobní data. Takto přenášené dokumenty musejí být odpovídajícím způsobem zabezpečeny před ztrátou, zpřístupněním nebo poškozením a musejí být řádně evidovány.
g) Omezení přístupu k OÚ prostřednictvím vymezení kompetencí v rámci organizační struktury zaměstnavatele, přičemž přístup k datům obecně je diferencován dle oddělení a pracovního zařazení. Statutární orgány mají přístup k veškerým datům a informacím.
h) Omezení přístupu k některým síťovým jednotkám, adresářům a aplikacím (programům) jen pro vymezený okruh oprávněných osob. Nastavení přístupů provádí IT pracovník výhradně na pokyn nadřízeného nebo statutárního zástupce. Požadavky zaměstnanců na nastavení oprávnění či přístupů k datům a aplikacím vyřizuje: *Pověřená osoba*.
i) Vzdělávání zaměstnanců. Zaměstnavatel zvyšuje povědomí odpovědných zaměstnanců školením o jejich povinnostech v souvislosti s ochranou subjektů údajů při zpracování jejich OÚ, zejména pak seznámením s obsahem tohoto vnitřního předpisu.
j) Služební (zaměstnavatelem svěřená) přenosná a periferní mobilní zařízení, jako jsou notebooky, chytré telefony a tablety, připojena na informační systémy, servery nebo do sítě zaměstnavatele např. za účelem vyřizování elektronické pošty jsou používána tak, že na každém z nich je nainstalován nejméně antivirový systém a zaměstnanci dodržují pokyny zaměstnavatele, IT správce a obecné zásady bezpečnosti spojené s přístupem do informačních systémů zaměstnavatele prostřednictvím těchto mobilních zařízení. Zaměstnanci jsou povinni zajistit nejméně v intervalu 6 měsíců kontrolu těchto zařízení IT pracovníkem. Tato zařízení nesmějí být využívána bez schválení statutárního zástupce pro soukromé účely nebo pro ukládání dat obsahující osobní údaje. Zaměstnanec je povinen zabezpečit svěřené zařízení před ztrátou, poškozením nebo přístupem třetí osobě. Zaměstnanec nesmí bez schválení statutárního zástupce a bez předchozí konzultace s IT pracovníkem připojit služební zařízení do cizí počítačové sítě (kabelové i bezdrátové sítě).
k) Soukromá přenosná a periferní mobilní zařízení, jako jsou notebooky, chytré telefony a tablety, nesmějí být bez předchozího souhlasu statutárního zástupce připojena na informační systémy, servery nebo do sítě zaměstnavatele. V případě takového schválení např. pro účely vyřizování elektronické pošty nebo přístupu k datům či aplikacím zaměstnavatele musí být na zařízení instalován nejméně antivirový systém a dostupné bezpečnostní aktualizace. Zaměstnanci dodržují pokyny zaměstnavatele, IT správce a obecné zásady bezpečnosti spojené s přístupem do informačních systémů zaměstnavatele prostřednictvím těchto mobilních zařízení. Zaměstnanci jsou povinni zajistit pravidelnou aktualizaci systému a nezbytných aplikaci pro eliminaci bezpečnostních rizik.
l) Bez závažného důvodu není povoleno tisknout citlivé osobní údaje! Veškeré dokumenty obsahující osobní údaje nebo jiné zneužitelné informace není možné tisknout na vzdálených tiskárnách (např. společné síťové tiskárny), pokud k nim nemá zaměstnanec okamžitý přístup nebo není nastaven zabezpečený tisk (vytištění dokumentu až po zadání osobního identifikačního čísla (PIN) nebo ověření uživatele čipem přímo na tiskárně). Není dovoleno ponechávat ve společných tiskárnách vytištěné dokumenty, je nutné je ihned odebírat.
m) V případě odesílání nebo přenášení elektronických dokumentů/dat obsahujících osobní údaje je nutné použít odpovídající zabezpečení (šifrování, zabezpečení dokumentů heslem, použití uzavřeného systému, např. datové schránky)

n) Pracovník odpovědný za přijímání nových zaměstnanců nebo za ukončování pracovního poměru musí vždy, pokud je to možné, nejdéle 3 dny před zahájením nebo ukončením pracovního poměru, nahlásit IT pracovníkovi údaje nezbytné k založení účtů a nastavení přístupů nebo blokaci stávajících oprávnění. Změny přístupů v případě omezení práv je nutné hlásit nejdéle 3 dny před termínem požadované změny.

2. Zaměstnanec je oprávněn předat OÚ jen zpracovateli, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření.

3. Zaměstnanec, který má poskytnout OÚ ke zpracování zpracovateli, je povinen prověřit, zda má zaměstnavatel se zpracovatelem uzavřenou písemnou smlouvu o zpracování osobních údajů a případně uzavření takové smlouvy iniciovat.

4. Zaměstnavatel provádí jednou ročně testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování OÚ.

5. Součástí pracovního nebo organizačního řádu případně pracovních smluv a pracovněprávních dohod zaměstnanců majících přístup k OÚ je doložka o mlčenlivosti a ochraně OÚ a součástí smluv se zpracovateli doložka obdobného obsahu. Popřípadě je v tomto smyslu uzavírána zvláštní dohoda o ochraně OÚ a mlčenlivosti.

6. Jakékoli porušení zabezpečení OÚ každý zaměstnanec neprodleně, nejpozději však do 24 hodin od okamžiku, kdy se o porušení dozvěděl, oznámí svému nadřízenému nebo Pověřené osobě, případně odpovědným osobám/statutárnímu zástupci uvedeným v odstavci IV. ODPOVĚDNÉ OSOBY tohoto předpisu.

7. Statutární zástupce nebo Pověřená osoba nejpozději do uplynutí 72 hodin od okamžiku, kdy byl bezpečnostní incident poprvé v organizaci zaznamenán, oznámí takové porušení zabezpečení/únik dat Úřadu. Proces oznámení konzultuje s DPO nebo pověří DPO řízením procesu oznámení incidentu Úřadu. Statutární zástupce dokumentuje veškeré případy porušení, účinky a přijatá nápravná opatření. Dojde-li k porušení zabezpečení OÚ zpracovávaných elektronicky, odpovědný zaměstnanec do 24 hodin informuje osobu, která spravuje informační systémy, aby zjistila narušitele a do 48 hodin navrhla nápravné opatření. Při řešení bezpečnostních incidentů zaměstnavatel spolupracuje se správcem sítě a pověřencem pro ochranu osobních údajů.

8. Pokud je pravděpodobné, že určitý případ porušení zabezpečení OÚ bude mít za následek vysoké riziko pro práva a svobody subjektu údajů, oznámí to pověřený zaměstnanec bez zbytečného odkladu subjektům údajů.

VII. ZVLÁŠTNÍ USTANOVENÍ

a) Zaměstnavatel je povinen jmenovat pověřence pro ochranu osobních údajů (DPO), neboť po provedené analýze sice neprovádí rozsáhlé pravidelné a systematické monitorování OÚ, ale současně je v pozici orgánu veřejné moci.

b) Zaměstnavatel dále není povinen provádět posouzení vlivu na ochranu OÚ, neboť není pravděpodobné, že druhy zpracování OÚ jím prováděné představují vysoké riziko pro práva a svobody subjektů údajů, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování OÚ.

VIII. ZPŮSOBY SLEDOVÁNÍ A MONITORINGU

Obecné podmínky provozování kamerového systému

1. Zaměstnavatel informuje touto cestou zaměstnance o existenci a provozování kamerového systému v prostorách chodeb, sborovny a koncertních sálů.

2. Zaměstnavatel monitoruje vymezené prostory z důvodu bezpečnosti a zdraví žáků, zaměstnanců a třetích osob pohybujících se ve sledovaných prostorách, dále pak za účelem ochrany majetku před protiprávním jednáním.

3. Hlavními právními důvody provozování kamerového systému a pořizování záznamů jsou ochrana životně důležitých zájmů subjektu, veřejný zájem a oprávněný zájem správce (právem chráněné zájmy zaměstnavatele), a to především za účelem ochrany života a zdraví fyzických osob, bezpečnosti a ochrany zdraví při práci, všeobecné ochrany majetku zaměstnavatele, ochrany před krádeží, před zneužitím a získávání důkazních materiálů pro orgány činné v trestním řízení, případně pro jiné orgány veřejné moci.

4. Správcem osobních údajů je zaměstnavatel. Zaměstnavatel nepověřil žádného zpracovatele, např. provozovatele PCO, aby pro něj zpracovával osobní údaje z kamerového systému.

Způsob zpracování OÚ

1. Jednotlivé kamery jsou umístěné ve výše uvedených prostorách.

   Kamery jsou umístěny mimo běžný dosah osob pohybujících se v sledovaných prostorech, kdy přístup k těmto kamerám má statutární zástupce organizace a správce kamerového systému v případě poruchy či nutnosti jiného zásahu z jeho strany.

   Rozvody kamerového systému jsou vedeny pomocí strukturované kabeláže v chráněných trasách.

   Záznamové zařízení a počítačová technika napojená na kamerový systém jsou umístěny v prostorách určených zaměstnavatelem v uzamykatelné místnosti s odpovídajícím zabezpečením a s omezeným počtem osob oprávněných ke vstupu, přičemž je současně vedena evidence osob majících přístup.

   Osobami, které mají k záznamům kamerového systému přístup, jsou statutární zástupce organizace, ad hoc na pokyn statutárního zástupce IT pracovník, a dále pak orgány veřejné moci, zejména pak orgány činné v trestním řízení.

   K záznamům se používá systém Hikvision jako součást síťového úložiště NVR. Pro kopírování nebo výmaz dat se používají nástroje k tomu určené přímo v aplikaci. Uložení záznamu se následně provádí do umístění, které je definováno prohlížečem, přes který se systém spravuje. Přístupová práva jsou nastavena jmenovitě přímo v systému, dokumentování nakládání se zpracovanými údaji je zajištěno v systému prostřednictvím funkce logování. Zabezpečení systému je pomocí silného hesla administrátora. Softwarové zabezpečení je zajištěno pravidelnými updaty, které vydává výrobce systému.

   a. Záznamy kamerového systému jsou zaměstnavatelem uchovávány po dobu maximálně 30 dnů (v závislosti na pohybu v budově a kapacitě záznamového zařízení je doba uložení typicky 2-3 týdny), což je nezbytná doba sloužící k odhalení konkrétního protiprávního jednání, krádeže apod. Následně dochází k jejich automatickému výmazu.

   b. Kamerový systém je zaměstnavatelem využíván ve veřejně přístupných prostorách. V místech, která jsou určena k soukromým účelům zaměstnanců (toalety, sprchy, prostory k převlékání), se tento kamerový systém nevyužívá. Použití kamerového systému na těchto místech je přísně zakázáno.

c. Všechna monitorovací zařízení včetně záznamu z kamerového systému jsou chráněna před přístupem neoprávněných osob, před zničením či zneužitím celého systému nebo záznamů.

d. O přístupu k záznamům kamerového systému jsou pořizovány elektronické záznamy v provozním deníku kamerového systému, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Provozní deník kamerového systému vede a spravuje statutární zástupce školy v elektronické podobě.

e. Prostory, které jsou zaměstnavatelem monitorovány, jsou označeny zřetelným nápisem umístěným v monitorované místnosti nebo před ní (informační cedule). Podrobná informace o zpracování osobních údajů je k dispozici u ředitele školy, na což je v rámci informačních cedulí upozorněno.

Práva a povinnosti subjektu údajů

1. Subjekty údajů mají právo na předložení podrobné informace o kamerovém systému, která obsahuje následující údaje:
   - Účely zpracování
   - Rozsah zpracování a kategorie osobních údajů
   - Identifikaci společnosti coby správce
   - Místo zpracování
   - Příjemce zpřístupněných údajů (orgány činné v trestním řízení)
   - Počet kamer
   - Popis rozmístění kamer ve sledovaných prostorech
   - Doba uchování záznamů vč. způsobu výmazu po uplynutí doby
   - Režim fungování kamer
   - Kontaktní údaje pro přijímání žádostí

   Podrobná informace je k dispozici u statutárního zástupce k nahlédnutí.

2. Subjekty osobních údajů mají vedle ostatních práv dle Nařízení také právo na poskytnutí záznamu z kamerového systému. Při poskytování záznamů z kamerového systému subjektům údajů společnost stanoví následující postup:
   - Kontaktní osoba (DPO, Pověřená osoba nebo statutární zástupce) převezme žádost;
   - Kontaktní osoba provede posouzení oprávněnosti žádosti;
   - V případě kladného vyhodnocení kontaktní osoba zajistí pořízení kopie záznamu. V případě negativního vyhodnocení s odůvodněním žádost zamítne;
   - V případě žádosti orgánů veřejné moci zajistí kontaktní osoba předání kopie záznamu příslušným orgánům (správní úřady, orgány činné v trestním řízení);
   - Kontaktní osoba vypracuje o každém pořízení kopie záznamu a jeho předání oprávněné osobě příslušný záznam, např. v provozním deníku kamerového systému nebo formou předávacího protokolu, který bude obsahovat: datum poskytnutí záznamu, zdůvodnění poskytnutí záznamu, identifikaci žadatele o záznam, specifikaci poskytnutých záznamů, identifikaci předávající a přejímající osoby;
   - Žádosti o kopii záznamu budou zpravidla vyřizovány ve lhůtě 2-3 týdnů od přijetí žádosti, případně ve lhůtě požadované orgány veřejné moci;
   - Subjektům údajů jsou vydávány toliko záznamy, resp. jejich části, na kterých jsou subjekty (žadatelé) samotné, přičemž jiné subjekty musí být nerozpoznatelné (např. formou rozostření obrazu);
   - Zaměstnavatel má právo požadovat přiměřenou úhradu nákladů spojených s poskytnutím kamerového záznamu, které činí paušální poplatek ve výši 500 Kč za hodinu záznamu z jedné kamery (poplatek spojený s anonymizací/pseudonymizací záznamu – rozmazání identifikačních znaků dalších osob na záznamu).

Sledování provozu mobilních telefonů a pevných telefonních linek

a. Zaměstnavatel provádí sledování provozu mobilní a pevné telefonie formou podrobných výpisů o uskutečněných hovorech a odeslaných zprávách.

Sledování provozu počítačové sítě a přístupů do informačních systémů

a. Zaměstnavatel provádí sledování počítačové sítě a přístupů do informačních systémů formou sběru logů a datových paketů o přístupu na síťová úložiště, přihlášení uživatelů do informačních systémů, provozu internetu a e-mailové komunikace.

b. Probíhá pouze nezbytný sběr dat nutných pro vyhodnocení případných bezpečnostních incidentů. Neprovádí se sběr obsahu komunikace.

IX. LHŮTY PRO VÝMAZ

1. Lhůty pro výmaz OÚ se řídí právní řádem České republiky a případně spisovým řádem zaměstnavatele. Není-li lhůta pro výmaz upravena zákonem ani není přijat spisový řád, pak platí, že skartační doba je 3 roky.

X. ÚČINNOST

Tento vnitřní předpis nabývá účinnosti dne 1. 9. 2024, přičemž byl zveřejněn způsobem, který je v souladu s příslušnými ustanoveními zákoníku práce, vč. seznámení zaměstnanců s jeho obsahem.

V Polici nad Metují dne 16. 8. 2024