Směrnice školy č. 17/18/05 o ochraně osobních údajů a nakládání s nimi

Směrnice o ochraně osobních údajů a 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).

1. Působnost

1.1 Tato směrnice upravuje postupy školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji, pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů 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"]. Směrnice rovněž upravuje některé povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji.

1.2 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.

1.3 Organizace při zpracovávání osobních údajů může vystupovat jako:

- správce osobních údajů, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za ně,
- zpracovatel osobních údajů, který zpracovává osobní údaje na základě zvláštního zákona nebo pověření správce.

1.4 Tato směrnice je závazná pro všechny zaměstnance školy. Směrnice je závazná i pro další osoby, které mají se školou jiný právní vztah (smlouva o dílo, dohoda o provedení práce, dohoda o pracovní činnosti, nájemní smlouva) a které se zavázaly postupovat podle této směrnice.

2. Vymezení odpovědnosti

2.1 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:

- plnění informační povinnosti k subjektům údajů,
- uplatňování práv subjektů údajů,
- zajištění technických a organizačních opatření na ochranu osobních údajů,
- spolupráce s pověřencem pro ochranu osobních údajů.

2.2 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.

2.3 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.

2.4 Moravskoslezský kraj jako zřizovatel organizace poskytuje metodickou pomoc v oblasti ochrany osobních údajů.

3. Zásady nakládání s osobními údaji

Při nakládání s osobními údaji se škola, její zaměstnanci a další osoby řídí těmito zásadami:

- Postupovat při nakládání s osobními údaji v souladu s právními předpisy,
- S osobními údaji nakládat uvážlivě, v souladu a míře se souhlasem se zpracováním osobních údajů,
- Zpracovávat osobní údaje ke stanovenému účelu a ve stanoveném rozsahu a dbát na to, aby tyto byly pravdivé a přesné,
- Zpracovávat osobní údaje v souladu se zásadou zákonnosti – na základě právních předpisů, při plnění ze smlouvy, při plnění právní povinnosti správce, při ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (zejména nezletilých), při ochraně oprávněných zájmů školy, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,
- Respektovat práva člověka, který je subjektem údajů, zejména práva dát a odvolat souhlas se zpracováním, práva na výmaz, namítat rozsah zpracování apod.,
- Poskytovat při zpracování osobních údajů zvláštní ochranu dětem,
- Poskytovat informace o zpracování osobních údajů, komunikovat,
- Při uzavírání smluv a právním jednání postupovat se zřetelem na povinnost chránit osobní údaje před zneužitím,
- Spolupracovat s pověřencem pro ochranu osobních údajů.

4. Postupy školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji

4.1 Škola všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Přitom škola především uchovává osobní údaje v prostorách, na místech,

v prostředí nebo v systému, do kterého má přístup omezený, předem stanovený a v každý okamžik alespoň řediteli školy známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením ředitele školy nebo jím pověřené osoby. Data obsahující osobní údaje uložená v počítačové síti jsou pravidelně a plánovaně zálohována. Zařízení, které zpracovávají osobní údaje nebo slouží k jejich uložení, jsou chráněna antivirovým, případně dalším bezpečnostním softwarem, a jsou dále chráněna tak, aby k nim neměli přístup neoprávněné osoby. Servery a další významné součásti počítačové sítě školy jsou umístěny v uzamčené místnosti s omezeným přístupem pouze osobám pověřeným ředitelem školy. Pro uložení dat obsahujících osobní údaje slouží výhradně zařízení v evidenci školy (např. externí disky, flashdisky apod.)

4.2 Škola zavede taková opatření, aby o nakládání a zpracování osobních údajů měl přehled alespoň ředitel školy nebo jím pověřená osoba a pověřenec pro ochranu osobních údajů. Mezi tato opatření patří např. ústní nebo písemná informace, písemná komunikace, stanovení povinností v pracovní smlouvě, v dohodě o provedení práce, v dohodě o pracovní činnosti, ve smlouvě, kterou škola uzavírá se třetí osobou (nájemní smlouva, smlouva o dílo, smlouva o poskytování služeb).

4.3 Škola alespoň jednou za rok provede zhodnocení postupů při nakládání a zpracování osobních údajů. Zhodnocení může být provedeno dle zvyklostí školy, zpravidla se učiní stručný záznam např. v zápisu z porady. Zjistí-li se, že některé postupy školy jsou zastaralé, zbytečné nebo se neosvědčily, učiní škola bezodkladně nápravu.

4.4 Každý zaměstnanec školy při nakládání s osobními údaji respektuje jejich povahu, tedy že jde o součást soukromí člověka jako subjektu údajů, a tomu přizpůsobí úkony s tím spojené. Zaměstnanec zejména osobní údaje nezveřejňuje bez ověření, že takový postup je možný, nezpřístupňuje osobní údaje osobám, které neprokáží právo s nimi nakládat. Zaměstnanec, vyplývá-li taková povinnost z jiných dokumentů, informuje subjekt údajů o jeho právech na ochranu osobních údajů; jinak odkáže na ředitele školy nebo jím určenou osobu nebo na pověřence pro ochranu osobních údajů.

4.5 Škola při nakládání a zpracovávání osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů.

4.6 Škola ihned řeší každý bezpečnostní incident týkající se osobních údajů, a to v součinnosti s pověřencem pro ochranu osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, především konkrétního žáka, studenta, zaměstnance, zákonného zástupce atd., škola tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepíše záznam. O každém závažném incidentu škola informuje Úřad pro ochranu osobních údajů.

4.7 Vzhledem k tomu, že škola eviduje v podstatě údaje o žácích a zaměstnancích, které stanovují právní předpisy (zejména školský zákon a pracovněprávní předpisy), nemá oznamovací povinnost vůči Úřadu pro ochranu osobních údajů podle ustanovení 3.6 věty první.

4.8 Organizační opatření k ochraně osobních údajů ve škole:

4.8.1 Třídní výkazy, katalogové listy a další materiály ze školní matriky, které obsahují osobní údaje žáků, jsou uloženy v uzamykatelných místnostech školy (kabinety, sborovna školy). Vyučující jednotlivých předmětů zapisují jen klasifikaci dle úvazku. Třídní výkazy, katalogové listy, další materiály ze školní matriky či jejich části nelze vynášet ze školy, předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.

4.8.2 Elektronická školní matrika je vedena v zabezpečeném informačním systému Bakaláři. Do tohoto systému mají přístup jednotliví pedagogové školy a další osoby, a to jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením. Při práci s elektronickou evidencí nesmí oprávněné osoby opouštět počítač bez odhlášení se nebo uzamčení zařízení, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přihlašovacího hesla; a v případě nebezpečí jeho vyzrazení jej ihned změnit. Přístupy nastavuje pověřený zaměstnanec školy – správce operačních systémů, který nastavuje potřebné zabezpečení dat a školní počítačové sítě (dle pokynů ředitele a zástupce ředitele). Zákonní zástupci žáků a žáci mají zajištěn zabezpečený dálkový přístup každý zvlášť a výhradně k vlastním údajům o klasifikaci na základě přihlašovacího kódu a hesla předaného správcem operačních systémů přísně individuálně:

- Pro zákonné zástupce žáků i žáky, kteří jsou přijati ke studiu, jsou přihlašovací kódy a hesla předány na třídních schůzkách nastupujících ročníků nebo na začátku školního roku.
- V případě ztráty nebo nutnosti změny hesla je toto možné provést použitím funkce Zapomenuté heslo ve webové aplikaci Bakaláři. Pro zajištění funkčnosti musí mít žák vyplněn správně svůj kontaktní email a zákonný zástupce žáka kontaktní email na zákonného zástupce. Změnu hesla lze provést také osobně u správce operačních systémů školy, a to opět zvlášť pro žáka a zákonného zástupce žáka. Na emailové nebo telefonické žádosti nebude brán zřetel.

Žádným způsobem nebudou ukládány nebo vytvářeny kopie, které obsahují čitelné přihlašovací údaje a hesla, s výjimkou dočasných souborů určených pouze pro přenos do jiných aplikací (školní jídelna, přístupový systém, e-learningový systém apod.).

4.8.3 Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních na sekretariátu školy, přístup k nim má ředitel školy nebo zástupce ředitele a personalistka.

4.8.4 Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni, zpravidla na poradě.

4.8.5 Zaměstnanci školy neposkytují bez právního důvodu žádnou formou osobní údaje zaměstnanců školy a žáků cizím osobám a institucím, tedy ani telefonicky ani mailem ani při osobním jednání.

4.8.6 Písemná hodnocení a posudky, která se odesílají mimo školu, např. pro potřeby soudního řízení, přijímacího řízení, pro zákonem nebo vyhláškou nařízené sběry dat vyplývajících z právní povinnosti, zpracovávají zaměstnanci určení ředitelem školy. Nejsou však oprávněni samostatně tato hodnocení podepisovat, poskytovat a odesílat jménem školy a mají povinnost zachovávat mlčenlivost o dané věci.

4.8.7 Seznamy žáků se nezveřejňují, neposkytují bez vědomého souhlasu žáků či zákonných zástupců žáků jiným fyzickým či právnickým osobám nebo orgánům, které neplní funkci orgánu nadřízeného škole nebo nevyplývá-li to ze zákona.

4.8.8 V propagačních materiálech školy, ve výroční zprávě či ročence školy, na školním webu či na nástěnkách ve škole apod. lze uveřejňovat výhradně textové či obrazové informace o jejich úspěších (např. u soutěží umístění na předních místech) s uvedením pouze jména (případně ročníku či třídy). Při publikování v tisku se autor dotazuje na souhlas příslušného žáka. Žák nebo zákonný zástupce má právo požadovat bezodkladné zablokování či odstranění informace či fotografie či záznamu týkající se jeho osoby, který zveřejňovat nechce. Platí to i o fotografiích či záznamech žáka bez uvedení jména v rámci obecné dokumentace školních akcí a úspěchů.

4.8.9 Psychologické, lékařské a jiné průzkumy a testování mezi žáky, jejichž součástí by bylo uvedení osobních údajů žáka, lze provádět jen se souhlasem žáka nebo zákonného zástupce žáka. To se netýká anonymních průzkumů, které však musí souviset se vzděláváním na dané škole a musí s ním předem písemně souhlasit ředitel či zástupce ředitele; to platí zvláště v případě, že výsledky jsou poskytovány mimo školu.

4.8.10 Pokud jsou pro vedení dokumentace využívány formuláře a software, je nutné provést kontrolu, zda nepožadují či nenabízejí evidenci nadbytečných údajů a tyto údaje nezpracovávat.

4.8.11 Ve škole se provozují kamerové systémy sledující prostory používané žáky a zaměstnanci školy v době, kdy jsou žáci přítomni ve škole, a to pouze z důvodu bezpečnosti žáků a zaměstnanců nebo ochrany majetku školy.

4.8.12 Uzavírá-li škola jakoukoli smlouvu (nájemní smlouvu, smlouvu o dílo, smlouvu o poskytnutí služeb, nepojmenovanou smlouvu apod.), k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, škola vždy a bezpodmínečně bude trvat na tom, aby ve smlouvě byla druhé smluvní straně uložena povinnost:

- přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,
- nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu školy,
- zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
- zajistit, aby se osoby oprávněné zpracovávat osobní údaje u dodavatele byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
- zajistit, že dodavatel bude škole bez zbytečného odkladu nápomocen při plnění povinností školy, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje školu,
- po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí škole a vymaže existující kopie apod.,
- poskytnout škole veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené škole právními předpisy,
- umožnit kontrolu, audit či inspekci prováděné školou nebo příslušným orgánem dle právních předpisů,
- poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví škola, součinnost potřebnou pro plnění zákonných povinností školy spojených s ochranou osobních údajů, jejich zpracováním,
- poskytnuté osobní údaje chránit v souladu s právními předpisy,
- přiměřeně postupovat podle této směrnice, která je přílohou smlouvy.

5. Pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů.

5.1 Škola nakládá a zpracovává pouze osobní údaje, které:

- souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, se sociálním, a zdravotním pojištěním (např. dosažené vzdělání, délka praxe, funkční zařazení apod.),
- souvisejí s jednoznačnou identifikací zákonných zástupců žáků v souladu se zákonem (jméno, příjmení, bydliště, kontakt, např. telefonní číslo pro případ nutného kontaktu školy se zákonným zástupcem v rámci ochrany zdraví, bezpečnosti a práv žáka, další údaje nezbytné např. pro vydání správního rozhodnutí apod.),
- související s identifikací žáka ze zákona (datum narození, místo narození, rodné číslo, státní příslušnost, bydliště, údaj o zákonném zástupci, soudní rozhodnutí vztahující se k přidělení dítěte do výchovy, nutný zdravotní údaj apod.),
- jsou nezbytné pro plnění právní povinnosti, ochranu oprávněných zájmů školy nebo ve veřejném zájmu,
- k jejichž zpracování získala souhlas subjektu údajů.

5.2 Osobní údaje se uchovávají pouze po dobu, která je nezbytná k dosažení účelu jejich zpracování, včetně archivace.

5.4 K osobním údajům mají přístup osoby k tomu oprávněné zákonem nebo na základě zákona. Do jednotlivých dokumentů školy, které obsahují osobní údaje, mohou nahlížet

- do osobního spisu zaměstnance vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele (§ 312 zákoníku práce),
- do údajů žáka ve školní matrice pedagogičtí pracovníci školy (v rozsahu daném pedagogickou funkcí), sekretářka,
- do údajů o zdravotním stavu žáka, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv výchovný poradce, vedoucí pedagogičtí pracovníci, třídní učitel, trenér nebo jiný ředitelem školy pověřený pracovník,
- do spisu, vedeném ve správním řízení účastníci správního řízení, sekretářka a personalistka, vedoucí pedagogičtí pracovníci (ředitel, zástupce ředitele, vedoucí vychovatel), osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.

6. Souhlas ke zpracování osobních údajů

6.1 Ke zpracování osobních údajů nad rozsah vyplývající ze zákonů (ze zákona vyplývá i oprávněný zájem, plnění právní povinnosti, plnění smlouvy, veřejný zájem) je nezbytný souhlas osoby, o jejíž osobní údaje se jedná. Souhlas musí být poučený, informovaný a konkrétní, nejlépe v písemné podobě. Souhlas se získává pouze pro konkrétní údaje (určené např. druhově), na konkrétní dobu a pro konkrétní účel.

6.2 Souhlas se získává pro zpracování osobních údajů jen tehdy, pokud je jejich zpracování nezbytně nutné a právní předpisy jiný důvod pro toto zpracování nestanoví.

6.3 Souhlas se poskytuje podle účelu např. na celé období školní docházky na škole, na školní rok, na dobu školy v přírodě apod. Udělený souhlas může být v souladu s právními předpisy odvolán.

7. Některé povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji

7.1 Každý zaměstnanec školy je povinen počínat si tak, aby neohrozil ochranu osobních údajů zpracovávaných školou.

7.2 Dále je každý zaměstnanec školy povinen:

- zamezit nahodilému a neoprávněnému přístupu k osobním údajům zaměstnanců, žáků, zákonných zástupců a dalších osob, které škola zpracovává,
- pokud zjistí porušení ochrany osobních údajů, neoprávněné použití osobních údajů, zneužití osobních nebo jiné neoprávněné jednání související s ochranou osobních údajů, bezodkladně zabránit dalšímu neoprávněnému nakládání, zejména zajistit znepřístupnění, a ohlásit tuto skutečnost řediteli školy či jinému příslušnému zaměstnanci.

7.3 Ředitel školy je povinen:

- informovat zaměstnance o všech významných skutečnostech, postupech nebo událostech souvisejících s nakládáním s osobními údaji ve škole, a to bez zbytečného odkladu,
- zajistit, aby zaměstnanci školy byli řádně poučeni o právech a povinnostech při ochraně osobních údajů,
- zajišťovat, aby zaměstnanci školy byli podle možností a potřeb školy vzděláváni nebo proškolováni o ochraně osobních údajů
- zajistit, aby škola byla schopna řádně doložit plnění povinností školy při ochraně osobních údajů, které vyplývají z právních předpisů.

8. Závěrečná ustanovení

Tato směrnice nabývá účinnosti dne 25. 5. 2018.

Tato směrnice nahrazuje veškeré přechozí směrnice, vnitřní předpisy a jiné dokumenty související s ochranou osobních údajů, které byly vydány organizací.

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 Ostravě dne 25. 5. 2018

Mgr. Václav Štencel
ředitel gymnázia

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 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:

- popis povahy bezpečnostního incidentu (popis co a kde se stalo),
- uvedení data a hodiny vzniku či zjištění bezpečnostního incidentu (popis kdy se stalo),
- popis kategorií osobních údajů, které jsou bezpečnostním incidentem ohroženy (citlivé osobní údaje, osobní údaje nezletilých apod.),
- alespoň přibližný počet subjektů údajů, které mohou být bezpečnostním incidentem ohroženy (nelze-li určit přesně aspoň přibližný počet),
- 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:

- datum a čas zjištění incidentu,
- datum a čas kontaktování pověřence,
- popis bezpečnostního incidentu dle odstavce 5 tohoto postupu,
- popis důsledků bezpečnostního incidentu,
- informace o posouzení rizika posouzení rizika pověřencem, příp. pověřencem Moravskoslezského kraje,
- popis případných přijatých opatření v souvislosti s řešením bezpečnostního incidentu,
- 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:

- popis povahy bezpečnostního incidentu (co kdy a kde se stalo),
- kontaktní údaje pověřence pro ochranu osobních údajů (jméno, e-mail, telefon),
- popis pravděpodobných důsledků bezpečnostního incidentu,
- popis opatření, která již byla organizací přijata nebo jsou navržena k přijetí s cílem vyřešit daný bezpečnostní incident.

Mgr. Václav Štencel
ředitel gymnázia