Škola Matiční gymnázium, Ostrava, Dr. Šmerala 25	
Směrnice k nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES	
Č. j.: GMAT/1671/2018	Účinnost od: 25. 5. 2018
Spisový znak:	Skartační znak: A10
Změny:	

Směrnice Matičního gymnázia, Ostrava, příspěvková organizace, Dr. Šmerala 25, 728 04 Ostrava k naplnění **nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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 „nařízení“), které spolu se zákonem o zpracování osobních údajů (jehož návrh je aktuálně v legislativním procesu) nahradí dosavadní právní úpravu, tj. zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

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. Směrnice rovněž upravuje některé povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji. Směrnice doplňuje systém směrnic platných v této oblasti na MGO.
1.2 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, nájemní smlouva) a které se zavázaly postupovat podle této směrnice.
1.3 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.
1.4 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.

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 Odpovědnou osobou dle předchozího odstavce tohoto článku směrnice je zástupce ředitele PaedDr. Karel Mohelník.
2.4 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.
Moravskoslezský kraj jako zřizovatel organizace poskytuje metodickou pomoc v oblasti ochrany osobních údajů.

3. Zásady nakládání s osobními údaji

3.1 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, souhlas se zpracováním osobních údajů nenadužívat,
- 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 děti požívají vyšší ochrany), 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.
4.2 Škola dodržuje taková opatření, aby o nakládání a zpracování osobních údajů bylo plně v souladu s naplnění **nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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)**
4.3 Škola alespoň jednou za rok provede zhodnocení postupů při nakládání a zpracování osobních údajů. Kontrola o hodnocení bude prováděna v souladu s **nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.**
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 jen ty 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.

5. Organizační opatření k ochraně osobních údajů ve škole

5.1 Třídní výkazy, katalogové listy a další materiály ze školní matriky, které obsahují osobní údaje žáků, jsou trvale uloženy v uzamykatelných skříních v kanceláři školy, a to v kanceláři ředitele nebo zástupců ředitele školy či na sekretariátu školy (viz platné směrnice MGO). Třídním učitelům jsou zapůjčeny na nezbytně dlouhou dobu k provedení zápisů. Vyučující jednotlivých předmětů zapisují jen klasifikaci dle úvazku a výhradně způsobem, který zajišťuje ochranu těchto údajů (viz operační systém Bakalář). 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.
5.2 Elektronická školní matrika je vedena v zabezpečeném informačním systému Bakalář. Do tohoto systému mají přístup jednotliví pedagogové školy a další osoby, a to v souladu s organizační strukturou školy a jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením. Při práci s elektronickou evidencí oprávnění nesmí oprávněné osoby opouštět počítač bez odhlášení se, nemohou nechat nahlížet žádnou jinou neoprávněnou osobu a musí chránit utajení přihlašovacího hesla; a v případě nebezpečí jeho vyzrazení jej ihned (ve spolupráci se správcem sítě) změnit. Přístupy nastavuje pověřený zaměstnanec školy – správce počítačové sítě, 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 výhradně k vlastním údajům o klasifikaci na základě přihlašovacího kódu a hesla přiděleného správcem počítačové sítě přísně individuálně prostřednictvím třídních učitelů.
5.3 Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních na sekretariátu MGO, přístup k nim má ředitel školy nebo zástupce ředitele, zastupuje-li ředitele, případně, je-li to nutné též sekretářka školy nebo mzdová účetní.
5.4 Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni při vzniku zaměstnaneckého poměru a pro projednávání všech případných změn.

5.5 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.
5.6 Písemná hodnocení a posudky, která se odesílají mimo školu, např. pro potřeby soudního řízení, přijímacího řízení, zpracovávají zaměstnanci určení ředitelem školy. Nejsou však oprávněni samostatně tato hodnocení podepisovat, poskytovat a odesílat jménem školy (není-li tento postup schválen vedením školy) a mají povinnost zachovávat mlčenlivost o dané věci.
5.7 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.
5.8 V propagačních materiálech školy, ve výroční zprávě či ročence školy, na školním webu či na nástěnkách ve škole apod. lze s obecným souhlasem žáků nebo zákonných zástupců žáků uveřejňovat výhradně textové či obrazové informace o jejich úspěších (např. u soutěží umístění na předních místech) s uvedením 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.
5.9 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 nim předem písemně souhlasit ředitel či zástupce ředitele; to platí zvláště v případě, že výsledky jsou poskytovány mimo školu.
5.10 Pokud jsou pro vedení dokumentace využívány formuláře a software, je nutné vždy provést kontrolu, zda nejsou požadovány nadbytečné údaje a tyto údaje nezpracovávat.
5.11 V budově školy se neprovozují kamerové systémy sledující prostory používané žáky a zaměstnanci školy v době, kdy jsou žáci přítomni ve škole.
5.12 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.

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

6.1 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.
6.2 Osobní údaje se uchovávají pouze po dobu, která je nezbytná k dosažení účelu jejich zpracování, včetně archivace a v souladu s platnou legislativou ČR.
6.3 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,
- do spisu, vedeném ve správním řízení účastníci správního řízení, sekretářka, vedoucí pedagogičtí pracovníci (ředitel, zástupce ředitele, vedoucí vychovatel), osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.

7. Souhlas k zpracování osobních údajů

7.1 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.
7.2 Souhlas se získává pro zpracování osobních údajů jen tehdy, pokud je jejich zpracování nezbytně nutné a právní předpisy jiný důvod pro toto zpracování nestanoví.
7.3 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.

8. Povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji

8.1 Každý zaměstnanec školy je povinen počínat si tak, aby neohrozil ochranu osobních údajů zpracovávaných školou.
8.2 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.
8.3 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.
8.4 Veškeré osobní údaje, které zaměstnanec MGO zpracovává v souladu se zákony, vyhláškami a normami, musí být administrovány pouze na technickém zařízení v majetku školy. Jakákoliv forma přenositelnosti je přísně zakázána.

9. Hlášení narušení bezpečnosti osobních údajů

Zjištění bezpečnostní události

- Hlášení bezpečnostní události nebo incidentu odpovědné osobě nebo pověřenci pro ochranu osobních údajů – **kontaktním místem pro hlášení o narušení bezpečnostních údajů je sekretariát MGO nebo pověřenec MGO;**
- vyhodnocení zdroje informace o narušení (interní, externí atd.);
- vyhodnocení základních informací;
- rozhodnutí o klasifikaci (událost nebo incident).

Reakce na bezpečnostní události a incidenty

- Událost:
  - odpovědná osoba/pověřenec pro ochranu osobních údajů událost vyšetří;
  - konfrontace události s historií událostí (opakovaná nebo nahodilá událost);
  - návrh opatření k nápravě;
  - ukončení šetření události.
- Incident:
  - svolání odpovědných osob souvisejících s řešením incidentu;
  - pokud je možné, tak realizace okamžité nápravy (zastavení provozu, zablokování práv atd.);
  - identifikace typu osobních údajů, u kterých došlo k porušení bezpečnosti;
  - přibližný rozsah údajů;
  - identifikace pravděpodobného zdroje úniku, narušení;
  - popis pravděpodobných důsledků dopadů na subjekty údajů;
  - vyhodnocení rizika dopadů na práva a svobody subjektů údajů:
    - bez rizika;
    - riziko;
    - vysoké riziko.
  - kontaktování odpovědné osoby z vedení SŠ;
  - rozhodnutí v případě vyhodnocení:
    - rizika - ohlášení dozorového úřadu;
    - vysokého rizika - ohlášení dozorového úřadu a oznámení subjektům údajů.
  - návrh nebo přijatá nápravná opatření k snížení dopadů na práva subjektů údajů,
  - návrh nebo přijatá nápravná opatření k eliminaci příčiny porušení bezpečnosti osobních údajů,
  - zpracování a odeslání hlášení dozorovému úřadu podle výše vyhodnoceného rizika.

9.1. Řešení bezpečnostního incidentu

- další vyšetřování incidentu na základě návrhů uvedených v hlášení dozorovému úřadu,
- návrh a přijetí dalších nápravných opatření,
- kontrola účinnosti přijatých opatření.

10. Rozhodovací proces při uplatňování práv subjektů údajů

10.1 Právo být informován o zpracování osobních údajů

Právo být informován o zpracování osobních údajů – rozumí se právo subjektu na určité informace o zpracování jeho osobních údajů. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů. Jedná se o tzv. pasivní právo, jelikož aktivitu musí vůči subjektu údajů vyvinout správce, aby požadované informace stanovené v GDPR subjektu údajů poskytl (při shromažďování osobních údajů od subjektu údajů – viz čl. 13 GDPR), resp. zpřístupnil (v případě, že osobní údaje nebyly získány od subjektu údajů – viz čl. 14 GDPR).

10.1.1 rozhodovací proces:

- Pokud jsou osobní údaje shromažďovány od subjektu údajů:
  - posoudit, vzhledem k účelu zpracování, pro který účel jsou osobní údaje shromažďovány, které informace dle § 13 GDPR je nutno subjektu údajů sdělit (informace se sdělit nemusí, pokud subjekt údajů již tyto informace má, a do té míry, v níž je má) a jakým způsobem;
  - sdělit či poskytnout subjektu údajů informace v rozsahu a způsobem dle předchozího odstavce již při shromažďování osobních údajů.
- Pokud osobní údaje nebyly získány od subjektu údajů:
  - posoudit, vzhledem k účelu zpracování, pro který jsou osobní údaje zpracovávány, nutnost poskytnout subjektu údajů informace a jejich rozsah (informace se sdělit nemusí, pokud subjekt údajů již tyto informace má, nebo kdy zaznamenání či zpřístupnění osobních údajů je výslovně stanoveno právními předpisy, nebo kdy poskytnutí těchto informací subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí) a jako formou (písemně či ústně);

- poskytnout subjektu údajů informace v rozsahu a formou dle předchozího odstavce:
  - v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
  - nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo
  - nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

10.2 Právo na přístup k osobním údajům

Právo na přístup k osobním údajům – tímto se rozumí právo získat od správce informaci (potvrzení), zda jsou či nejsou osobní údaje subjektu údajů zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování;
- kategorie dotčených osobních údajů;
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
- plánovaná doba, po kterou budou osobní údaje uloženy;
- existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku;
- právo podat stížnost u dozorového úřadu;
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

10.2.1 rozhodovací proces:

- ověřit totožnost tazatele, který uplatňuje své právo. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje tazatele v SŠ zpracovávány;
- pokud ano, poskytnout tazateli tuto informaci a současně, pokud to tazatel požaduje, poskytnout informace v požadovaném rozsahu (kopii zpracovávaných údajů), max. však v rozsahu uvedeném v předchozím;
- pokud ne, poskytnout tazateli informaci, že jeho osobní údaje nejsou předmětem zpracování osobních údajů v SŠ.

10.3 Právo na opravu nepřesných osobních údajů

Právo na opravu nepřesných osobních údajů – toto právo neznamená povinnost SŠ aktivně vyhledávat nepřesné údaje (nic tomu však nebrání), ani to neznamená povinnost například každoročně požadovat po subjektu údajů aktualizaci jeho údajů. Pokud se subjekt údajů domnívá, že správce zpracovává jeho nepřesné údaje, upozorní jej na to.

10.3.1 rozhodovací proces:

- ověřit totožnost osoby, která uplatňuje právo na opravu údajů, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit skutečný stav (přesnost) dotčených zpracovávaných osobních údajů subjektu údajů;
- dle potřeby vyžadovat od subjektu údajů relevantní doklad stvrzující avizovanou nepřesnost ve zpracování osobních údajů;
- dle doloženého stavu nepřesné zpracovávané osobní údaje opravit.

10.4 Právo na výmaz (být zapomenut)

Právo na výmaz (být zapomenut) – znamená povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování;
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
- osobní údaje byly zpracovány protiprávně;

- osobní údaje musí být vymazány ke splnění právní povinnosti;
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 GDPR.

10.4.1 rozhodovací proces:

- ověřit totožnost osoby, která uplatňuje právo na výmaz, tj. zda se skutečně jedná
- o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje subjektu údajů v SŠ zpracovávány, pro jaké účely a na základě jakého právního důvodu (viz čl. 6 GDPR);
- posoudit nebo vyhodnotit zpracování osobních údajů, kdy je splněna alespoň jedna z uvedených podmínek – u těchto zpracování osobní údaje subjektu údajů zlikvidovat (v listinné i elektronické formě);
- u zpracování, kde nelze uplatnit ani jednu z uvedených podmínek, osobní údaje nelikvidovat.

10.5 Právo na omezení zpracování

Právo na omezení zpracování – toto právo lze vnímat jako „právo dočasné“. Subjekt údajů může uplatnit toto své právo v případech:

- pokud popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- pokud je zpracování protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

10.5.1 rozhodovací proces:

- ověřit totožnost osoby, která uplatňuje právo na omezené zpracování, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda nastala jedna z výše uvedených podmínek pro uplatnění práva;
- pokud bylo zpracování omezeno:
    - mohou být dotčené osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo důležitého veřejného zájmu;
    - je nutno upozornit subjekt údajů, který dosáhl omezení zpracování, na to, že bude omezení zpracování zrušeno.
- Způsoby omezení zpracování osobních údajů:
    - dočasný přesun vybraných údajů do jiného systému zpracování;
    - znepřístupnění vybraných osobních údajů uživatelům;
    - dočasné odstranění zveřejněných údajů z internetových stránek;
    - v systémech automatizovaného zpracování zajistit, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny.

10.6 Právo na přenositelnost

Právo na přenositelnost – podstatou uplatnění tohoto práva je možnost za určitých podmínek získat osobní údaje, které se týkají subjektu údajů a které správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, například JSON, CSV, TXT, a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby správce předal jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jinému správci, je-li to technicky proveditelné.

Pro uplatnění tohoto práva musí být současně splněny dvě podmínky:

- musí jít o zpracování založené na právním základu souhlasu či smlouvě;
- zpracování se provádí automatizovaně.

10.6.1 rozhodovací proces:

- ověřit totožnost osoby, která uplatňuje právo na přenositelnost údajů, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje subjektu údajů v SŠ zpracovávány, pro jaké účely, na základě jakého právního důvodu (viz čl. 6 GDPR) a v jaké formě (manuální nebo listinná, automatizovaná nebo elektronická);
- pokud jsou splněny společné podmínky uvedeny výše, postupovat podle formulace požadavku subjektu údajů na uplatnění tohoto práva.

10.7 Právo vznést námitku

Právo vznést námitku – subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na základě právních důvodů:

- zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

10.7.1 Rozhodovací proces:

- ověřit totožnost osoby, která vznáší námitku proti zpracování osobních údajů, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje subjektu údajů v SŠ zpracovávány, pro jaké účely a na základě jakého právního důvodu;
- pokud je zpracování založeno na některém ze dvou právních důvodů uvedených výše, posoudit nebo vyhodnotit, zda existují nebo neexistují závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků;
- v návaznosti na posouzení nebo vyhodnocení skutečností dle předchozího odstavce osobní údaje dále zpracovávat nebo nezpracovávat.

Pozn.: námitku lze vznést i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nelze již jeho osobní údaje pro tento účel zpracovávat.

10.8 Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování

Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování – toto právo zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Automatizované rozhodování je přípustné v případě, kdy je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem, pokud je povoleno právem EU nebo členským státem nebo pokud je založeno na výslovném souhlasu subjektu údajů.

10.8.1 rozhodovací proces:

- ověřit totožnost osoby, která uplatňuje toto právo, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou v SŠ zpracovávány osobní údaje subjektu údajů způsobem, který by byl v rozporu s tímto právem;
- pokud ano, takové zpracování osobních údajů ukončit.

10.9 Společná ustanovení k rozhodovacím procesům

- s výjimkou práva být informován o zpracování osobních údajů musí být informace
- o přijatých opatřeních žadateli (subjektu údajů) poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit

o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení;

- informace, veškerá sdělení a provedené úkony na žádost subjektu údajů se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce;
- o zneužití práva subjektem údajů se jedná zejména tehdy, pokud se žádosti opakují a jsou zjevně nedůvodné či nepřiměřené. V takovém případě může správce uložit přiměřený poplatek nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost dokládá správce;
- pokud subjektem údajů požadovaná opatření nebyla správcem přijata, musí správce bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti informovat subjekt údajů o důvodech nepřijetí těchto opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

10.10 Organizační a technická opatření související s ochranou osobních údajů

- 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.
- Organizace je povinna přijmout a dodržovat tato organizační opatření:
- Osoby provádějící zpracování osobních údajů mají stanoveny povinnosti ke zpracování osobních údajů, zejména prostřednictvím právních předpisů, pracovních smluv a jiných vnitřních předpisů organizace.
- Dochází-li ke zveřejňování dokumentů, obsahujících osobní údaje je nutné provést anonymizaci osobních údajů, ledaže je jejich zveřejnění stanoveno zvláštním právním předpisem.
- Organizace je povinna přijmout a dodržovat tato personálně-organizační opatření:
- 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.
- 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.
- Organizace je povinna přijmout a dodržovat tato administrativně-organizační bezpečnostní opatření:
- 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.
- 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.
- 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.
- Dokumenty obsahující osobní údaje jsou ukládány tak, aby nedošlo ke zneužití osobních údajů, a to zejména uložením v uzamykatelných místnostech či skříních.
- Organizace při manipulaci s dokumenty postupuje dle platného spisového a skartačního řádu.
- Organizace je povinna přijmout a dodržovat tato opatření v oblasti zabezpečení prostředků výpočetní techniky:
- 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.

- 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.
- 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.
- Zařízení dle písm. a) musí být chráněna antivirovým a antimalware softwarem, případně dalším bezpečnostním softwarem.
- Data uložená v počítačové síti a zařízeních jsou pravidelně a plánovaně zálohována a uchovávána.
- 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.
- Přístup externích osob do počítačové sítě, informačního systému či aplikace je umožněn pouze osobám, na základě schválení ředitele organizace či osoby pověřené ředitelem organizace.
- Organizace je povinna přijmout a dodržovat tato kontrolní opatření:
- 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.
- Organizace je povinna při realizaci kontrolních opatření dle písm. a) tohoto odstavce spolupracovat také s pověřencem a Moravskoslezským krajem jako zřizovatelem organizace.

10.11 Nově aplikované administrativní operace na MGO:

- jedno vstupní místo pro žádosti o uplatňování jednotlivých práv – sekretariát školy (je možno se přímo obrátit na pověřence pro ochranu osobních údajů)
- jedno výstupní místo zpět k subjektům údajů – sekretariát školy (je možno se přímo obrátit na pověřence pro ochranu osobních údajů).
- 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

Platnost směrnice: od 25. 5. 2018

S touto směrnicí byli zaměstnanci MGO seznámeni 15. 5. 2018 (viz podpisová listina)

Mgr. Ladislav Vasevič
ředitel MGO

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.