MASARYKOVA
OBCHODNÍ AKADEMIE
RAKOVNÍK

2. 1. Směrnice
pro nakládání s osobními údaji pro školu

Směrnice pro nakládání s osobními údaji

1. JAK SE SMĚRNICÍ NAKLÁDAT

		Poznámky a příklady
1.1.	Tuto Směrnici mohou ředitelé škol, zejména základních a mateřských, a dalších školských zařízení, především v malých obcích, využít buď tak, jak je, anebo s přihlédnutím k potřebě jednoduchosti a konkrétních instrukcí zaměstnancům a dalším osobám její pasáže včlenit do pracovního nebo organizačního řádu nebo přímo do některých smluv a pracovních náplní. Konkrétní provedení by měli konzultovat s Pověřencem pro ochranu osobních údajů.	Směrnice se zařadí mezi další interní směrnice ve škole. Levý sloupec obsahuje normativní text směrnice, pravý sloupec uvádí příklady, nebo podrobněji popisuje jednotlivá ustanovení směrnice.
1.2.	Směrnici vydává ředitel. Zřizovatel[1] zajistí, aby Směrnicí byli vázáni rovněž členové školské rady nebo rady školy, kteří nepodléhají řediteli.	Ředitel podepíše a předloží zaměstnancům k seznámení. Nechá je podepsat, že se se směrnicí seznámili a zavazují se k jejímu dodržování. Zřizovatel to stejné udělá se zástupci zřizovatele a rodičů ve školské radě.

2. PŘEDMĚT SMĚRNICE A ZÁKLADNÍ USTANOVENÍ

		Poznámky a příklady
2.1.	Touto směrnicí škola **Masarykova obchodní akademie, Rakovník, Pražská 1222** (dále jen „škola“) stanovuje vnitřní pravidla pro zajištění ochrany osobních údajů a plnění povinností podle Obecného nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů jakožto přímo účinného předpisu EU (dále jen „Obecné nařízení“) a podle zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon“), zejména při zpracování osobních údajů vykonávaných školou, jejími zaměstnanci, případně dalšími osobami.	Upozorňujeme, že dřívější zákon č. 101/2000 Sb., o ochraně osobních údajů byl zrušen. Pokud na něj máte ve svých formulářích odkaz, nahraďte ho odkazem na Obecné nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR) a na zákon č. 110/2019 Sb., o zpracování osobních údajů.
2.2.	Ustanovení této směrnice jsou závazná pro všechny osoby v rámci školy, zejména pro zaměstnance školy (dále „zaměstnanci“). Obdobně jako pro zaměstnance je tato směrnice závazná i pro členy školské rady, resp. rady školy[2] (dále „školská rada“), dále osoby, které mají se školou jiný právní vztah (smlouva o dílo, nájemní smlouva) a které se zavázaly postupovat podle této směrnice, především pokud se při své činnosti seznamují, případně zpracovávají osobní údaje školy jako správce údajů.	Jedná se např. o dodavatele služeb – pravidelný IT servis softwaru; školitel bezpečnosti a ochrany zdraví při práci; externí účetní a další.

[1] Zřizovatel zřizuje školskou radu, jedině on tedy může směrnicí zavazovat její členy, kteří nejsou zaměstnanci školy (§ 167 odst. 2 školského zákona).

[2] V případě školské právnické osoby, § 130 školského zákona.

2.3.	Jakékoliv smlouvy, podle kterých osobní údaje zpracovávají či se při plnění smlouvy s osobními údaji seznamují další osoby, (dále jen "zpracovatelé a další smluvní osoby"), musejí být písemné (včetně elektronické formy). Pokud smluvní vztah (např. standardní smluvní dokumenty dodavatele) neobsahuje závazek k ochraně osobních údajů alespoň v rozsahu, upraveném touto směrnicí, musí obsahovat závazek k dodržování této směrnice, konkretizaci povinností podle směrnice a potvrzení, že smluvní strana se se směrnicí seznámila.	Bakaláři a další poskytovatelé softwaru a online služeb s cloudovými službami; externí účetní; poskytovatelé cloudových služeb a další.
2.4.	Pokud pro školu zajišťuje zpracování osobních údajů v rámci plnění smluvních povinností jiný subjekt (zpracovatel), pak musí být v rámci smluvních vztahů zaručeno plnění povinností podle Obecného nařízení a ve smyslu předchozího bodu též této směrnice a musí být upravena odpovědnost za tyto činnosti vůči správci a vůči kontrolním orgánům. Náležitosti smlouvy o zpracování osobních údajů upravuje Obecné nařízení.	Bakaláři a další poskytovatelé softwaru a online služeb s cloudovými službami; externí účetní; poskytovatelé cloudových služeb a další. Smlouva o zpracování osobních údajů obsahuje zejména: popis povahy zpracování a jednotlivé činnosti zpracování; prohlášení zpracovatele o schopnosti dostát souladu s Obecným nařízením; závazek mlčenlivosti, a to i po ukončení smlouvy či pracovního vztahu; zpracovávat osobní údaje pouze na pokyn správce; bez souhlasu správce nevyužívat služby jiného zpracovatele; popis zabezpečení osobních údajů při zpracování.

3. ZÁKLADNÍ POJMY

		Poznámky a příklady
Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon. V souladu s tím je		
3.1.	**osobním údajem** jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;	
3.2.	**citlivým osobním údajem** osobní údaj vypovídající 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. Osobní údaje týkající se rozsudků v trestních věcech a trestných	Členství v odborech; zdravotnická dokumentace; informace o alergiích a jiných zdravotních omezení; podávání léků; údaje o národnosti; víře (někdy uvedené nadbytečně v životopise); otisk prstu; portrét použitý pro identifikaci osoby kamerou. Citlivým osobním údajem není rodné číslo, to však neznamená, že ho lze volně používat!

činů se pro účel této směrnice hodnotí obdobně jako citlivé osobní údaje;	
3.3. **zpracováním osobních údajů** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, která je prováděna 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; za zpracování osobních údajů se nepovažuje:	
3.3.1. pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu (vzdělávací a výchovné, kulturní, společenské, sportovní akce, schůze), aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje[3];	Momentky z běžných činností ve škole; na zahradě apod.; video a fotografie z veřejné akce; fotografie vítězů na webu školy; obce nebo v obecním a školském zpravodaji.
3.3.2. běžné nahodilé používání jednotlivých osobních údajů v rámci vzdělávání a výchovy, včetně nahodilého hodnocení žáků;	Známkování a hodnocení práce před spolužáky; výběr dětí na školní soutěž.
3.4. **subjektem údajů** fyzická osoba, k níž se osobní údaje vztahují;	Žák; dítě; rodič; zaměstnanec; podnikající fyzická osoba; smluvní partner.
3.5. **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;	V praxi se jedná o část formuláře *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při zahájení školní docházky.
3.6. **likvidací osobních údajů** fyzické zničení jejich nosiče nebo jejich fyzické vymazání. K fyzickému vymazání nepostačuje vymazat data ze souboru nebo soubor z adresáře.	Skartování dokumentů včetně mazání dokumentů z počítače. Dokumenty uložené v elektronické podobě jsou fakticky zničeny: fyzickou destrukcí nosičů (pokud jde o CD, DVD); použitím software zabezpečující vymazání. V tomto případě nesmí jít o pouhé smazání dokumentů z adresáře, protože i poté by byla možná obnova smazaných souborů. Musí jít o opakované přepsání původních souborů novými údaji.

4. OSOBNÍ ÚDAJE A JEJICH ZPRACOVÁNÍ

	Poznámky a příklady
4.1. **Způsob zpracování osobních údajů a pověřené osoby**	

[3] Stanovisko ÚOOÚ č. 12/2012–K použití fotografie, obrazového a zvukového záznamu fyzické osoby

4.1.1. Osobní údaje lze zpracovávat pouze za podmínek stanovených Obecným nařízením, případně zvláštními zákony, přičemž je nezbytné dodržovat ustanovení této směrnice. Zpracovávat lze pouze osobní údaje získané zákonným způsobem.	Konkrétně se jedná o čl. 6 Obecného nařízení. Nezákonný způsob zpracování je např. uchovávání kopií rodných listů dětí zaměstnanců; kopírování občanských průkazů; využívání e-mailových adres zákonných zástupců k zasílání marketingových sdělení od firem, které se školou spolupracují, pokud k tomu zákonní zástupci předem nedali souhlas.
4.1.2. Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou:	
4.1.2.1. zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů;	Ředitel; zástupce ředitele; účetní; mzdová účetní; pedagog; vychovatel; metodik prevence; vedoucí školní jídelny a další.
4.1.2.2. člen školské rady, pokud je to nezbytné pro výkon jeho funkce;	Zástupce z řad rodičů, zřizovatele a školy.
4.1.2.3. osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.	Jedná se o zpracovatele (viz bod 2.3) - např. externí účetní; IT; poskytovatel cloudového úložiště a další.
4.2. Účel zpracování, zákonnost a nově zaváděné účely zpracování[4]	
4.2.1. Veškerá zpracování osobních údajů probíhají v rámci jednotlivých agend, tzv. „účelech zpracování“. Ten, kdo rozhoduje o činnosti zpracování (dále jen „odpovědný zaměstnanec (garant)“), pro každé zpracování (agendu, evidenci) stanoví účel zpracování, tedy jeho výstižný a konkrétně vymezující popis v rozsahu několika slov. O účelu drobných zpracování (tj. zpracování s nízkým rizikem[5], např. pomocné a dočasné evidence menšího počtu žáků, zaměstnanců, dodavatelů apod., bez citlivých osobních údajů) rozhoduje osoba, do jejíž kompetence spadá úkol, který zpracování osobních údajů vyžaduje. V případě, kdy lze předpokládat, že účel zpracování zasahuje subjekty osobních údajů ve velkém rozsahu, je povinna předložit stanovení účelu k rozhodnutí řediteli.	Účelem je často název agendy – vedení školní matriky; evidence strávníků; evidence členů Spolek Rady rodičů; evidence vypůjčených školních pomůcek žákům; seznam žáků s vybranými penězi na výlet a další.
4.2.2. Právní titul či tituly[6] každého účelu zpracování určí odpovědný zaměstnanec (garant). V případě, kdy agenda obsahuje také citlivé osobní údaje, určí zároveň právní titul pro citlivé údaje. K obojímu určí také právní	Citlivé osobní údaje viz bod 3.2 - např. individuální vzdělávací plány; katalogové listy; žádosti o přijetí v případě, že obsahují popis zdravotního omezení dítěte/žáka.

[4] Čl. 5 odst. 1 písm. a) a b) Obecného nařízení

[5] Čl. 33 odst. 1 ON, případy, kdy není pravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob

[6] Právním titulem, někdy nazývaný také “právní důvod”, je některé ustanovení čl. 6 odst. 1 písm. a) až f) , čl. 9/2 písm. a) až j) , čl. 10 Obecného nařízení.

	základ[7], je-li potřebný. Pokud je právním titulem souhlas subjektu údajů, jeho znění se vždy konzultuje s pověřencem. Právními tituly jsou zpravidla:	
	● plnění právní povinnosti;	Agendy, jednoznačně vyplývající ze zákona – dokumentace školy podle § 28 školského zákona (školní matrika); osobní spisy zaměstnanců podle zákoníku práce; dokumentace v oblasti BOZP; vedení účetnictví; spisová služba; evidence projektů (Šablony) a další.
	● plnění úkolu ve veřejném zájmu;	Agendy, které nejsou v zákoně jednoznačně uloženy, ale vyplývají z obecných úkolů, stanovených zákonem nebo jiným obecně závazným předpisem. Jedná se např. o vedení kroniky školy; hodnocení zaměstnanců; záznam z hodnocení a provedených kontrol; vedení pomocné evidence v jídelně o počtu vydaných obědů u zaměstnanců a cizích strávníků; vedení pomocné evidence dětí/žáků k účasti na akcích, k platbám a další.
	● plnění smlouvy;	Osobní údaje nutné k uzavření pracovní smlouvy; osobní údaje nájemců školních prostor.
	● oprávněný zájem správce;	Nainstalovaná kamera pouze za účelem ochrany majetku, např. na zadní, nepoužívaný vchod do budovy.
	● výjimečně též souhlas subjektu údajů.	Pokud je pro zpracování osobních údajů nezbytný souhlas (dítě, jeho zákonný zástupce, zaměstnanec) pak musí být informovaný, konkrétní a písemný (viz bod 4.5.3). Zpracování osobních údajů je možné provádět až po získání souhlasu. Písemná podoba souhlasu se uchovává po celou dobu zpracování údajů. V praxi se jedná o část formuláře *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při zahájení školní docházky. Zveřejňování fotografií s uvedením jména, příjmení, věku a dalších osobních údajů dítěte/žáka/zaměstnance; zakládání e-mailových účtů v Google nebo Microsoft.
4.2.3.	Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu a navrhne nezbytný rozsahu údajů pro dané zpracování, dobu a způsob uchování a způsob informování subjektů údajů.	Učitel chce zřídit pro žáky novou internetovou službu s jejich registrací; ředitel chce vytvořit přehled žáků nebo učitelů, v němž bude shromažďovat údaje pro jejich hodnocení; škola začne poskytovat novou službu, např. posilovnu, a zřídí evidenci uživatelů a další.
4.2.4.	Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec (garant) vyžádá posouzení pověřencem.	

[7] Právním základem je konkrétní ustanovení právního předpisu ČR, o které se v daném případě zpracování opírá. Právní základ je potřebný u právních titulů podle čl. 6/1 písm. c) a e) ON. Dále též u některých právních titulů pro citlivé osobní údaje podle čl. 9/2 ON.

4.2.5. O každém nově zamýšleném účelu zpracování, vyjma drobných zpracování, jak jsou uvedena v bodu 4.2.1, je ten, kdo navrhuje jeho účel, povinen informovat pověřence, a to před jakýmkoliv krokem. Zahájit novou činnost zpracování lze jen na základě doložitelného posouzení pověřencem.	Tato povinnost jednoznačně vyplývá z čl. 38 odst. 1 Obecného nařízení.
4.2.6. Pověřené osoby jsou povinny zpracovávat osobní údaje pouze ke stanovenému účelu, v rozsahu pracovní náplně a úkolů, které jim byly stanoveny jejich nadřízenými anebo vyplývajícím z jejich funkce nebo smlouvy, a na místech k tomu určených. Jsou povinny dodržovat základní zásady při zpracování osobních údajů.	Např. mzdová účetní má přístup pouze k personalistice a podkladům pro mzdy; vedoucí stravování pouze k seznamu strávníků a popř. bankovnímu účtu speciálně pro stravné či k evidenci školného v MŠ; v rámci Bakalářů se obvykle ředitel dostane do všech modulů a učitelé mají oprávnění editovat a doplňovat pouze informace svých tříd.
4.2.7. Ustanovení tohoto článku se při výkonu jeho funkce přiměřeně vztahuje i na člena školské rady, který spolupracuje s odpovědným zaměstnancem (garant) a pověřencem, a to za podmínky, že není zaměstnancem.	
4.3. Zásady zpracování osobních údajů	
Pověřené osoby jsou povinny dodržovat tyto základní zásady při zpracování osobních údajů:	
4.3.1. zpracovávat osobní údaje korektním a transparentním způsobem;	Na webu jsou zveřejněny informace o zpracování, s podrobnými informacemi o jednotlivých agendách. Každý správce má toto v části „Informace o zpracování osobních údajů“, často (nesprávně) záložka „GDPR“[8].
4.3.2. před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování;	Uvedeno v komplexních kontrolních záznamech, které pomáhal vytvořit pověřenec (excel tabulka), viz bod 4.4.
4.3.3. zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu, včetně archivace v případech stanovených skartačním plánem, poté je likvidovat;	Např. výběrové řízení na nové zaměstnance: Po uchazečích jsou vyžadovány pouze údaje nezbytné pro posouzení vhodnosti uchazečů v rámci výběrového řízení. Další rozšiřující informace jsou požadovány až po případném rozhodnutí o uzavření pracovně právního vztahu. Osobní údaje neúspěšných uchazečů jsou skartovány a vymazány. V případě, že jsou uchovány pro využití při dalším výběrovém řízení, je subjekt údajů požádán o souhlas. Škola má aktualizovaný a platný spisový řád a skartační plán.
4.3.4. zpracovávat přesné osobní údaje a podle potřeby je aktualizovat. Třídní učitel má povinnost na začátku školního roku zkontrolovat aktuálnost údajů o žácích a jejich zákonných zástupcích, zejména je vyzvat k ohlášení změn (např. změna bydliště během prázdnin,	Zaměstnancům je v rámci porad a školení připomínána jejich zákonná povinnost informovat zaměstnavatele o změnách v jejich osobních údajích a také jejich právo nahlížet do svého osobního spisu.

[8] Označit Informace o zpracování osobních údajů jen zkratkou „GDPR“ nelze. Povinností správce je mimo jiné komunikovat srozumitelně a vyvarovat se používání zkratek a odborných výrazů. Zkratka „GDPR“ může být použita jen jako doplnění srozumitelného označení dané sekce jako je např. „Informace o zpracování osobních údajů“.

telefonního spojení apod.) v listinné i elektronické formě, jakož i při každé změně i v průběhu školního roku; přesnost údajů je zajištěna: ověřováním údajů poskytnutých subjektem, například porovnáním s osobními doklady, doklady o vzdělání; pravidelnými opakovanými kontrolami; aktivním dotazováním;	U dětí probíhá kontrola jejich osobních údajů každoročně při zahájení školního roku. Tím jsou o možnosti doplnění, opravy osobních údajů informováni i zákonní zástupci dětí. Zaměstnanci jsou při získávání údajů od dětí, jejich zákonných zástupců, od zaměstnanců, uchazečů či jiných osob povinni používat výhradně školou schválené formuláře, dotazníky a jiné texty.
4.3.5. zajišťovat náležité zabezpečení osobních údajů (viz bod 8).	Využití alespoň free antivirového programu; silná hesla; zamčené kanceláře či skříně; vymezené přístupy; organizační řád; aktualizované náplně práce zaměstnanců.
4.4. Záznamy o zpracování a komplexní kontrolní záznamy	
4.4.1. Každý odpovědný zaměstnanec (garant) vede v excelové tabulce jímž byla provedena implementace Obecného nařízení (dále jen „Komplexní kontrolní záznamy“):	Vedeno ve spolupráci s pověřencem, který pravidelně aktualizuje záznamy zpracování i komplexní kontrolní záznamy (excel tabulku).
4.4.1.1. záznamy o příslušných účelech zpracování (dále jen „záznam o zpracování“)[9];	Stručný výtah z excelové tabulky, tj. z komplexních kontrolních záznamů – dvanáct povinných údajů ke každé agendě.
4.4.1.2. záznamy o provedených opatřeních k dosažení souladu s Obecným nařízením jako je likvidace či výmaz dat, lhůty pro likvidaci, forma a lhůty zálohování, šifrování přenosných médií;	Každý výmaz, oprava, vyřízení požadavku subjektu údajů je vhodné poznamenat do komplexních kontrolních záznamů (excelová tabulka) k příslušné agendě dole do poznámek.
4.4.1.3. záznamy o bezpečnostních incidentech jako je únik, ztráta, neoprávněný přenos či zveřejnění;	Každý bezpečnostní incident je nutno poznamenat do komplexních kontrolních záznamů (excelová tabulka) k příslušné agendě dole do poznámek, a to i tehdy, když se nehlásil Úřadu.
4.4.1.4. další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektů údajů.	Do komplexních kontrolních záznamů (excelová tabulka) k příslušné agendě dole do poznámek je vhodné poznamenat i další aspekty, například o důvodu určitého postupu, aby bylo možné jej doložit.
4.4.2. Ke komplexním kontrolním záznamům mají přístup odpovědní zaměstnanci (garanti) a pověřenec. O změnách v komplexních kontrolních záznamech musejí odpovědní zaměstnanci (garanti) vždy informovat pověřence, např. sdílením aktualizované verze.	Ředitel, zástupce ředitele – obvykle osoba určená ke komunikaci s pověřencem.
4.4.3. Ředitel nebo jím určená osoba zajistí pravidelné zálohování komplexních kontrolních záznamů a případných souvisejících dokladů.	Lze požádat i pověřence.
4.5. Zveřejňování informací o subjektech údajů	

[9] Čl. 30 Obecného nařízení

4.5.1. Ve veřejně šířených informačních materiálech a prostředcích školy, například v ročence, na webu, ve školním zpravodaji se používají především takové ilustrativní fotografie/videa a související informace, které žáka/žákyni neidentifikují jednoznačně i pro cizí osoby[10], například celkové fotografie a záběry ze třídy, z akce, kde nejsou žáci/žákyně zobrazeni s podrobným portrétem a/nebo se neuvádí více, než křestní jméno. Takové zobrazení nevyžaduje svolení.	Momentky uvedené ve školním či obecním zpravodaji, na webu školy, obce – nejedná se o zpracování osobních údajů. V praxi se jedná o část formuláře *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při zahájení školní docházky (část "Informace").
4.5.2. V případech, kdy je to pro prezentaci žáka/žákyně vhodné, lze použít uvedené fotografie/videa tak, že lze určit totožnost, zejména uvedením jména a příjmení a/nebo podrobného portrétu, jde o zachycení podoby a její rozšiřování ve smyslu § 84 a 85 občanského zákoníku; takové použití vyžaduje svolení, které nemusí být písemné a může vyplývat ze situace. Od žáků mladších 15 let[11] je však nutné vyžádat od zákonného zástupce toto svolení anebo sdělení, že žákovi k němu udělil souhlas ve smyslu § 32 občanského zákoníku, a to na určené období až 5 školních roků (první stupeň, druhý stupeň), a to písemně anebo doloženým prohlášením, například na třídní schůzce na základě prezenční listiny[12].	Vítěz ve sběru; vítěz olympiády; zveřejnění jeho úspěchu v obecním zpravodaji a/nebo ve školském zpravodaji apod. V praxi se jedná o část formuláře *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při zahájení školní docházky (část "Svolení").
4.5.3. V případech zvláštních akcí pořádaných školou, kdy je to pro prezentaci žáka/žákyně vhodné, lze k takto zachycené podobě žáka/žákyně připojit ke jménu a příjmení další údaje, například o třídě, věku, účasti na akci konkrétního data, úspěchů ve vzdělání, vítězství v soutěžích včetně sportovních apod. V takovém případě jde o zpracování osobních údajů podle Obecného nařízení a pořízení a zveřejnění údajů vyžaduje souhlas ve smyslu čl. 4 bod 2 a 11 Obecného nařízení. Pro získání souhlasu platí totéž jako pro získání svolení podle předchozího bodu, souhlas musí být písemný, včetně elektronické formy.	V praxi se jedná o část formuláře *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při zahájení školní docházky (část "Souhlas").
4.5.4. Seznamy žáků se nezveřejňují, pokud nejde o zvláštní případ zpracování, pro který žáci nebo jejich zákonní zástupci dali souhlas.	Nezveřejňuje se tak na webu seznam dětí, které nastupují do první třídy, nebo rozdělení dětí do jednotlivých tříd. Přípustné je nechat takový seznam na začátku šk. roku na vstupních dveřích, ovšem jen po nezbytně nutnou dobu.

[10] Rozsudek NS 30 Cdo 936/2005: I. Podmínkou poskytnutí ochrany práva na podobu je, aby osoba zobrazeného byla na základě zobrazení obecně identifikovatelná.

[11] Ve skutečnosti mohou žáci v zásadě podle § 31 OZ tato svolení a souhlasy udělovat sami podle rozumové a volní vyspělosti, tedy podle situace asi od 13 let. Pro tuto směrnici se však pro jistotu stanoví napevno 15 let. (*§ 31 OZ: „Má se za to, že každý nezletilý, který nenabyl plné svéprávnosti, je způsobilý k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jeho věku.")*

[12] Například pokud se učitel na třídní schůzce dotáže rodičů, zda svolují s takovýmto používáním fotografií a videí, a nikdo neprojeví nesouhlas, pak je třeba to poznamenat k prezenční listině a tuto uchovat jako doklad. Toto svolení nelze zaměnit se souhlasem podle následujícího bodu č. 4.5.3.

5. DOKLADY SOULADU S OBECNÝM NAŘÍZENÍM

	Poznámky a příklady
5.1. Každá pověřená osoba, pokud to plyne z náplně její práce, dbá na uchování dokladů, opravňujících určité zpracování osobních údajů, jako jsou	
5.1.1. smlouvy, pro jejichž plnění se zpracovávají osobní údaje;	
5.1.2. doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu;	V praxi se jedná např. o zpracování osobních údajů pro plnění smlouvy, nebo o zpracování osobních údajů na základě souhlasu.
5.1.3. doklady o vyřízení žádostí subjektů údajů;	
5.1.4. souhlasy se zpracováním osobních údajů;	V praxi se jedná o část formuláře *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při zahájení školní docházky.
5.1.5. balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby;	V praxi při instalaci kamer se záznamem, nebo při instalaci zařízení při vstupu pomocí čipu. *(Upozorňujeme, že vstupní systémy fungující na principu biometrických údajů, např. otisk prstu nejsou přípustné!)*
5.1.6. evidence klíčů, je-li potřebná;	
5.1.7. evidence přístupů do počítačů a přístupových práv v informačním systému, je-li potřebná;	
5.1.8. údaje o zpřístupnění záznamu kamerového, docházkového systému, či dalších specifických záznamů osobních údajů;	
5.1.9. další obdobné doklady.	
5.2. Tyto doklady vede odpovědný zaměstnanec (garant) v komplexním kontrolním záznamu (excelová tabulka), pokud to jejich povaha umožňuje, jinak se v komplexním kontrolním záznamu pouze uvede, kde jsou uloženy.	

6. PRÁVA SUBJEKTŮ ÚDAJŮ

	Poznámky a příklady
6.1. **Informování subjektů údajů**[13]	
6.1.1. Odpovědný zaměstnanec (garant) zajistí informování subjektů údajů, jejichž údaje škola zpracovává, zejména na webu školy, případně při uzavření smlouvy nebo získání souhlasu se zpracováním. Zajistí též stručný,	Informace o zpracování na webu školy (výtah z komplexních kontrolních záznamů – excelové tabulky); informace o zpracování ve formuláři *Informace/Svolení/Souhlas v souvislosti s fotografiemi a videem*, který podepisují zákonní zástupci dětí/žáků při

[13] Čl. 13 a 14 Obecného nařízení

	transparentní, srozumitelný a snadno přístupný způsob těchto sdělení[14].	zahájení školní docházky, uvedení vět o zpracování osobních údajů na smlouvách apod.
6.1.2.	Odpovědný zaměstnanec (garant) zajistí také doložitelnost uvedeného informování. V rámci své kompetence může tento úkol uložit jinému zaměstnanci.	Informování probíhá nejčastěji v písemné podobě.
6.2.	**Přístup k osobním údajům[15]**	
6.2.1.	Požadavky subjektů údajů vyřizuje odpovědný zaměstnanec (garant), který může v rámci své kompetence tento úkol uložit jinému zaměstnanci. Pro vyřízení se přiměřeně postupuje podle obecného předpisu pro přístup k informacím (zákon č. 106/1999 Sb.), neuplatní se správní řád.	Využití dokumentu "*Postupy správce při splnění požadavků, plynoucích z práv subjektů údajů. Manuál pro školy a školská zařízení*".
6.2.2.	Požádá-li subjekt údajů o sdělení svých osobních údajů, ověří se totožnost žadatele a potvrdí na žádosti, případně se ověření totožnosti k žádosti přiloží, např. číslo průkazu, podle kterého byla ověřena, ověření uznávaného elektronického podpisu, datové schránky (dále jen „ověření totožnosti").	Žádost může subjekt údajů podat jakkoliv, včetně obyčejného e-mailu. Podle způsobu podání se následně přistoupí k potřebnému ověření totožnosti (ve formě výzvy).
6.2.3.	Běžné provozní dotazy týkající se osobních údajů (zejm. informace o zpracování osobních údajů), vyřídí zaměstnanec podle okolností co nejdříve.	
6.2.4.	K vyřízení ostatních žádostí o přístup k osobním údajům (zejm. export údajů) je příslušný odpovědný zaměstnanec (garant). Žádost se vyřídí do 30 dnů. Odesílané informace obsahují pouze odpovědi na kladené dotazy, jen v nezbytném rozsahu, uvádějí se pouze oficiálně zpracovávané informace (nikoli neoficiální, byť známé, např. o rodinném zázemí). Jakýkoli odesílaný text musí být schválen vedením školy či odeslán přímo vedením školy (například z e-mailu ředitele).	Zpravidla jsou informace poskytovány bezplatně, kromě případů, kdy správce posoudí žádost jako zbytečně opakovanou, nepřiměřenou, nedůvodnou, nebo pokud nejde o oprávněný zájem žadatele. Pokud je požadována úhrada, její výše se řídí sazebníkem o poskytování informací podle zákona č. 106/1999 Sb. o svobodném přístupu k informacím. Lhůta začíná běžet až od okamžiku, kdy – pokud to bylo nutné – žadatel vyhověl výzvě k ověření totožnosti nebo doplnil upřesnění žádosti.
6.2.5.	V případě potřeby a s ohledem na složitost a počet žádostí může odpovědný zaměstnanec (garant) prodloužit lhůtu vyřízení žádosti o další dva měsíce, přičemž o tom informuje subjekt údajů do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.	
6.2.6.	Jestliže subjekt údajů podává žádost v elektronické formě a je-li to možné, poskytnou se informace v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob.	

[14] Čl. 12 Obecného nařízení

[15] Čl. 15 Obecného nařízení

6.3. **Právo na výmaz, opravu a doplnění**	
6.3.1. Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů.	
6.3.2. Subjekt údajů má právo žádat výmaz, opravu a doplnění osobních údajů, které se ho týkají[16]. Případy, kdy je požadavek na výmaz oprávněný, stanoví čl. 17 odst. 1 a 3 Obecného nařízení. Žádost vyřídí odpovědný zaměstnanec (garant) po ověření totožnosti a po prověření oprávněnosti požadavku ihned, jakmile je to možné, nejdéle do 30 dnů; článek 6.2.5. Směrnice se použije obdobně. Pokud má ověření oprávněnosti požadavku trvat delší dobu, zejména by se osobní údaje dotčené žádostí měly zpracovávat ke stanovenému účelu zpracování (např. zaslat pravidelné vyúčtování s chybným údajem), zajistí jejich vyřazení ze zpracování [17] a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.	Podle čl. 17 Obecného nařízení má subjekt údajů právo na výmaz údajů, pokud již údaje nejsou potřebné pro původní účely, při odvolání souhlasu subjektu, při námitkách proti zpracování, při protiprávním zpracování, pokud není poskytnut souhlas se zpracováním, pokud je povinnost výmazu dána právní povinností. Výmaz se provádí na základě písemné žádosti, nelze ho provést u zpracování osobních údajů na základě právní povinnosti (pokud je dodržena skartační lhůta). Subjekt údajů má právo na opravu údajů, pokud jsou nepřesné, nebo neúplné. Na provedení opravy má škola nejdéle jeden měsíc, případně na vysvětlení, pokud oprava nebyla provedena. Škola předchází tomu, aby zpracovávané údaje byly neaktuální, údaje o žácích i zaměstnancích pravidelně ověřuje.
6.3.3. Oznámí-li subjekt údajů (např. telefonicky nebo e-mailem), že osobní údaje, které se ho týkají, se změnily, a nelze dostatečně ověřit jeho totožnost s ohledem na závažnost požadované změny (např. na základě znalosti e-mailové adresy), vyzve ho odpovědný zaměstnanec (garant) k postupu, jenž umožní totožnost ověřit.	Změna údajů o žákovi; změna příjmení; trvalé adresy apod.
6.3.4. Zjistí-li pověřená osoba při své činnosti, že při zpracování osobních údajů došlo ke zjevné chybě v psaní (např. překlepu), informuje odpovědného zaměstnance (garanta) a údaj opraví.	Chyba, která má za následek, že subjekt osobních údajů může být zaměnitelný s jinou osobou. Chyba se stane v přepisu rodného čísla apod.

7. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

	Poznámky a příklady
7.1. Pro školu zajišťuje pověřence společnost SMS-služby s.r.o. prostřednictvím svého zaměstnance, který je hlavní odpovědnou osobou ve vztahu ke škole pro výkon úkolů pověřence.	
7.2. Ředitel zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.	Informace o pověřenci musí být na webových stránkách školy – stačí e-mail a telefon, není nutné jméno a příjmení (je doporučované). Informace by měly být jednoduše dostupné, max. na 1–2 kliky. Část s informacemi o

[16] Čl. 16, 17 Obecného nařízení

[17] „omezení zpracování“

	zpracování osobních údajů a s informacemi o pověřenci doporučujeme nazvat jako "Informace o zpracování osobních údajů", viz bod. 4.3.1.
7.3. Všechny pověřené osoby jsou povinny[18]:	
7.3.1. konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením;	Zejména jakékoliv rozhodnutí vytvořit nové zpracování osobních údajů (novou agendu); použít na zpracování nové technické prostředky apod.
7.3.2. poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování;	
7.3.3. zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem;	
7.3.4. neukládat pověřenci úkoly, které by vedly k jeho střetu zájmů.	Například aby pro ně sám udělal ty činnosti, u kterých by zároveň měl nezávisle posuzovat jejich soulad s Obecným nařízením. Pověřenec může toliko poskytnout doporučení.
7.4. V případě řešení otázek o zpracování osobních údajů se zaměstnanci, žáci/žákyně, jejich zákonní zástupci a další osoby, jejichž osobní údaje škola zpracovává, obrací na pověřence s žádostí o radu, týkající se jejich osobních údajů.	O této možnosti je třeba je informovat.
7.5. Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě.	

8. BEZPEČNOST INFORMACÍ

8.1. **Obecné postupy při zabezpečení osobních údajů**	
8.1.1. Přiměřeně zabezpečeny musejí být zpracovávané osobní údaje, jakož i ty, které nejsou systematicky zpracovávané, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech.	E-maily v e-mailové schránce, včetně e-mailů pedagogů týkající se výuky v soukromém e-mailu; využití silných hesel; uspávání počítače po určité době neaktivity; šanony v uzavřených skříních; přehled o přístupech a klíčích do jednotlivých kanceláří školy apod.
8.1.2. Úroveň zabezpečení lze přiměřeně snížit u osobních údajů, u nichž je riziko pro subjekty údajů nepatrné nebo jsou běžně dostupné veřejnosti:	
8.1.2.1. na základě zákona o svobodném přístupu k informacím;	
8.1.2.2. na základě oprávněného zveřejnění (například ve veřejně přístupných registrech);	IČ; adresy firem; jména jednatelů a další.

[18] Čl. 38 Obecného nařízení

8.1.2.3. nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací.	E-mail v rámci třídy, kdo si ještě nevyzvedl školní práce na konci roku (jen několik příjmení).
8.1.3. V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.	
8.1.4. Osobní údaje musí být zabezpečeny před neoprávněným nebo nahodilým přístupem k nim, proti jejich změně, zničení či ztrátě (zejména dostatečné zálohování), neoprávněným a nezabezpečeným přenosům, proti jejich jinému neoprávněnému zpracování, jakož i proti jinému zneužití osobních údajů. Zabezpečení spočívá při nepřítomnosti pověřených osob zejména v uchovávání záznamových médií (listinných i elektronických), obsahujících osobní údaje, v uzamčených skříních, v uzamykání kanceláří a jiných míst.	Uzamčení zálohy dat, případně právní ošetření cloudu; zabezpečení el. zařízení (počítač, externí disk, flash disk atd.); antivirové programy; zabezpečené přístupy; přístup omezeného počtu osob a další.
8.1.5. Pověřené osoby jsou povinny dodržovat pravidla informační bezpečnosti, zejména nesmějí bez souhlasu správce informačního systému instalovat nedůvěryhodné programy (zejm. „zdarma“). Je zakázáno otevírat podezřelé odkazy nebo přílohy e-mailů. V případě nejasností je pověřená osoba povinna kontaktovat nadřízeného anebo správce informačního systému.	
8.1.6. Dále jsou pověřené osoby povinny vyvarovat se jakéhokoliv jednání, které by mohlo být chápáno jako neoprávněné zveřejňování osobních údajů nebo vést k neoprávněnému přístupu třetích osob k osobním údajům. Zejména, ale nikoliv pouze:	Neměly by se zveřejnit na sociálních sítích „historky ze školy“ obsahující osobní údaje.
8.1.6.1. sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem. Tím není dotčena možnost používat osobní údaje při běžné činnosti školy ve smyslu článku 3.3.1 (pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu (vzdělávací a výchovné, kulturní, společenské, sportovní akce, schůze), aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje,) a 3.3.2 (běžné nahodilé používání jednotlivých osobních údajů v rámci vzdělávání a výchovy, včetně nahodilého hodnocení žáků);	Vzdálená teta, nebo nový partner matky, který nemá žádný zákonný vztah k dítěti/žákovi.
8.1.6.2. hlasitě sdělovat podrobné osobní údaje ve veřejně přístupných prostorách (např. šatny, chodby, jídelna apod.);	Rozhovor učitelek o sociální situaci žáků, veřejně během služby na chodbách; jednání s rodiči o citlivých otázkách žáka v doslechu jiných osob.

8.1.6.3. umožnit nepovolaným osobám nahlížet do dokumentů s osobními údaji nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny, nechávat třetí osoby samotné v kabinetech nebo nechávat ve třídách dokumenty obsahující osobní údaje bez dozoru;	Ponechat sestavu osobních údajů v dosahu cizích osob (např. při třídní schůzce).
8.1.6.4. sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo zařízením, v případě jeho vyzrazení ihned zajistit jeho změnu.	Vyvarovat se např. zaznamenání si hesel na zadní stranu kalendáře nebo na monitor počítače; nalepení si hesla přímo na stůl nebo na spodní stranu police nad stolem.
8.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje	
8.2.1. Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být mimo dobu, kdy jsou pod dohledem zaměstnanců, zabezpečeny v uzamčených skříních, popř. na jiných místech, zajišťujících jejich ochranu. To platí i pro kopie písemností a digitální zálohy, obsahující osobní údaje.	Uzamčení zálohy dat, případně právní ošetření cloudu; zabezpečení el. zařízení (počítač, externí disk, flash disk atd.); antivirové programy; zabezpečené přístupy; přístup omezeného počtu osob a další. Záznamy obsahující citlivé osobní údaje (například o zdravotním stavu osob), jsou uloženy bezpečně v uzamčené skříni, ke které mají přístup pouze oprávněné osoby. Je také zajištěno jejich předávání pouze oprávněným orgánům.
8.2.2. Třídní knihy, výkazy, katalogové listy, individuální vzdělávací plány a další materiály ze školní matriky, které obsahují osobní údaje žáků, jsou trvale uloženy v uzamykatelných skříních v kanceláři školy, ředitele nebo zástupce ředitele (dále jen „kancelář“). Pokud je to nutné, mohou je v nezbytném rozsahu ukládat také třídní učitelky/učitelé v zamykatelných skříňkách ve třídě nebo kabinetu. Tyto materiály či jejich části nelze ponechávat bez dozoru, vynášet ze školy, předávat nebo jejich kopie poskytovat neoprávněným osobám.	Předávání údajů ze školní matriky je dáno právními předpisy (statistické výkaznictví), jiným subjektům jsou údaje poskytovány, pokud prokáží oprávněnost svého požadavku (soudy, policie, OSPOD…). Jsou stanovena odlišná oprávnění pro přístup k datům.
8.2.3. Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři, přístup k nim má ředitel školy nebo zástupce ředitele, zastupuje-li ředitele, případně, je-li to nutné, též sekretářka školy nebo mzdová účetní. Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu[19].	Pracovní smlouvy, dohody o provedení práce i dohody o pracovní činnosti a pracovní náplně všech zaměstnanců obsahují povinnosti zaměstnanců v oblasti GDPR. O zaměstnancích jsou shromažďovány pouze nezbytné údaje. Pokud jsou výjimečně pořizovány kopie dokumentů, kterými zaměstnanec dokládá určité skutečnosti (např. doklady o vzdělání), pak bez nadbytečných údajů. Pokud to není nezbytné, kopie dokumentů se nepořizují, údaje se jen ověří porovnáním s originálem (osobní doklady, rodné listy, rozsudky).

[19] § 312 zákoníku práce

8.2.4. Likvidace osobních údajů se provádí podle spisového řádu a skartačního plánu školy. Pokud skartace určitého typu osobních údajů není skartačním plánem upravena, likvidují se po uplynutí doby nezbytné k danému účelu. Osobní údaje se likvidují zároveň v listinné i elektronické formě, pokud jejich účely zpracování nejsou odlišné. Dokumenty uložené v elektronické podobě jsou zničeny fyzickou destrukcí nosičů, pokud jde o CD, DVD nebo použitím software zabezpečující vymazání.	Nesmí jít o pouhé smazání dokumentů v adresáři, protože i poté by byla možná obnova smazaných souborů, musí jít o opakované přepsání původních souborů novými údaji.
8.2.5. Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.	
8.3. Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích	
8.3.1. Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů. To platí i pro služební telefony, pokud obsahují osobní údaje zpracovávané v agendách školy podle článku 4.2.1. nebo k nim mají dálkový přístup.	Využití antivirových programů; silných hesel; heslování přístupu do externích disků; v případě notebooků šifrování disků; pravidelná obměna hesel. Prioritně využívání pracovních zařízení.
8.3.2. Počítače s přístupem k osobním údajům musejí mít alespoň zabezpečený přístup do počítače (přihlášení pod heslem) a nastaveno uzamčení obrazovky po době nečinnosti nejvýše 5 minut. Při odchodu z pracoviště (např. pauza na oběd) se oprávněná osoba odhlásí (např. klávesová zkratka Win+L).	Každý má u svého počítače (mobilního telefonu) přihlašovací heslo, které je dostatečně silné. Počítač se uspává v případě delší neaktivity.
8.3.3. Významné evidence osobních údajů (například mzdová, personální agenda, rozsáhlá evidence žáků s dalšími, zejména kontaktními údaji, záznamy z výchovných komisí, individuální vzdělávací plány) musejí být zabezpečeny také zvláštním přístupem do programového vybavení anebo být jako soubor šifrované.	
8.3.4. Elektronická školní matrika se vede v zabezpečeném informačním systému, do kterého mají přístup jednotliví pedagogové písemně pověření ředitelem, a to jen na základě jedinečného přihlášení a pouze v rozsahu oprávnění daného funkčním zařazením. Při práci s elektronickou evidencí nesmějí pověřené osoby opouštět počítač bez odhlášení. Přístupy nastavuje správce informačního systému podle pokynů ředitele a zástupce ředitele. Žáci a jejich zákonní zástupci mohou mít zabezpečený dálkový přístup na základě	Jsou stanovena odlišná oprávnění pro přístup k datům: Pedagogický pracovník má přístup pouze ke svému předmětu; třídní učitel má přístup ke všem známkám třídy a ke kompletní evidenci třídy; ředitel, případně zaměstnanec pověřený vedením dokumentace školy pak má přístup k celé matrice školy. Předávání údajů z matriky je dáno právními předpisy (statistické výkaznictví), jiným subjektům jsou údaje poskytovány, pokud prokáží oprávněnost svého požadavku (soudy, policie, OSPOD).

	jedinečného přihlášení výhradně k vlastním údajům o klasifikaci.	
8.3.5.	Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, úložiště souborů mobilního telefonu a podobně, musejí být, i když není určen k vynášení z objektu, alespoň:	
8.3.5.1.	zajištěna šifrováním disku či jiného úložiště pomocí šifrovacího programu;	
8.3.5.2.	zajištěna zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně;	
8.3.5.3.	být jako soubor šifrované, nebo	
8.3.5.4.	je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizována.	
8.3.6.	Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, úložiště souborů mobilního telefonu a podobně, které jsou vynášeny mimo pracoviště, zaměstnanec:	
8.3.6.1.	nesmí tuto techniku předávat třetím osobám;	
8.3.6.2.	musí učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávat ji bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.);	
8.3.6.3.	nesmí používat výpočetní techniku pro práci s daty školy na veřejných místech;	
8.3.6.4.	musí ztrátu či odcizení okamžitě nahlásit svému nadřízenému.	
8.3.7.	Pokud přenosné médium sloužilo jen k přenosu, musejí být data s osobními údaji bezodkladně po přenosu bezpečně fyzicky vymazána podle článku 3.6.	
8.3.8.	Před vyřazením jakéhokoliv elektronického nosiče dat (likvidace, prodej, výpůjčka, darování) musí být nosič zkontrolován a všechny osobní údaje bezpečně fyzicky vymazány podle článku 3.6.	
8.3.9.	Pověřené osoby pravidelně posuzují úroveň zabezpečení informačních systémů včetně přenosu dat s ohledem na rizika pro subjekty osobních údajů a v případě potřeby přijímají vhodná technická a organizační opatření, aby rizika zmírnily.[20]	

[20] Čl. 32 Obecného nařízení

8.3.10. Pověřené osoby zejména dbají na dostatečnou kvalitu hesel (nejméně 8 znaků, obsahuje minimálně 3 ze 4 položek: Velká písmena, malá písmena, čísla, symboly jako pomlčka či lomítko), pravidelné obměny hesel a je-li to možné vzhledem k nutné zastupitelnosti, důvěrnosti pouze pro jednoho uživatele. V případě potřeby ukládají hesla zabezpečeně a zcela odděleně od počítačů a médií, na nichž jsou použita.	Dobré je se vyvarovat např. jménům rodinných příslušníků a datům jejich narození. Nepřípustná jsou hesla jako 1234 nebo 77777.
8.3.11. Přenos souborů s osobními údaji nezabezpečenou sítí Internet (např. protokol http://) prostřednictvím běžné elektronické pošty a jejich uložení na nezabezpečených uložištích (běžné e-mailové schránky, přechodná úložiště jako Úschovna.cz) je přípustný jen v šifrované podobě minimálně v archivním souboru (např. ve formátu „zip“, „rar“, atd.) se zaheslováním souboru a předáním hesla příjemci jinou cestou, například SMS zprávou na ověřené číslo telefonu či pomocí jiné bezpečné aplikace. Šifrování však není nutné při předání datovou schránkou nebo zabezpečeným cloudem.	
8.3.12. Umožňuje-li to programové vybavení, odpovědné osoby (garanti) vždy využijí možnosti záznamu přístupů a činnosti (auditního záznamu, logu) na počítačích nebo v informačním systému. Záznamy pravidelně kontrolují. Tímto úkolem může být pověřen určený zaměstnanec.	
8.3.13. Počítačová (kybernetická) bezpečnost v organizaci je zajištěna na všech počítačích organizace:	
8.3.13.1. instalací antivirových programů;	
8.3.13.2. stanovením přístupových práv, hesel, zákazu sdílení hesel několika osobami;	
8.3.13.3. zajištěním automatických bezpečnostních aktualizací používaného software;	
8.3.13.4. při jakékoliv likvidaci hardware musí být znemožněna možnost získání osobních údajů;	
8.3.13.5. pravidelný servis a výpočetní techniky je zaměřen i na kontrolu oblasti bezpečnosti dat;	
8.3.13.6. je prováděno pravidelné testování přijatých technických a organizačních opatření;	
8.3.13.7. pravidelným školením zaměstnanců;	
8.3.13.8. vhodnou pracovní náplní metodika ICT (pokud v organizaci působí).	
8.3.14. Za plnění povinností stanovených v článku 8.3.13. jsou odpovědny odpovědné osoby (garanti) podle rozsahu svých oprávnění.	

8.3.15.	Zaměstnanec pomáhá zajišťovat kybernetickou bezpečnost na počítačích tím, že	
8.3.15.1.	provádí pravidelné zálohování dat, tak aby nedošlo k jejich ztrátě při případném odcizení či poruše počítače a byla zajištěna schopnost obnovy dat v případě fyzických či technických incidentů, ledaže je to uloženo jiné pověřené osobě;	
8.3.15.2.	používá pouze silná hesla;	
8.3.15.3.	maže a neotvírá nevyžádanou poštu, odmazává SPAM v emailové schránce i v počítačích.	

9. PORUŠENÍ ZABEZPEČENÍ A MÍRA JEHO RIZIKA

		Poznámky a příklady
9.1.	Vědomé porušení povinnosti mlčenlivosti, neoprávněné zveřejnění, sdělení, zpřístupnění a přisvojení osobních údajů zaměstnancem je porušení povinností, které mu vyplývají z pracovního poměru zvlášť hrubým způsobem. Při neoprávněném nakládání s osobními údaji může jít o trestný čin podle § 180 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů – jde o neoprávněné zveřejnění, zpracování, sdělení, zpřístupnění, přisvojení osobních údajů, porušení mlčenlivosti.	
9.2.	Zjistí-li kdokoliv, že došlo k fyzickému nebo elektronickému porušení zabezpečení osobních údajů, například úniku, ztrátě, zničení, neoprávněnému zveřejnění osobních údajů (dále jen „incident“), neprodleně o tom informuje ředitele, pověřence a odpovědného zaměstnance (garanta).	Zavirování počítače; odeslání e-mailu s více osobními údaji jinému adresátovi; smazání souborů s osobními údaji; otevření e-mailu, který má v sobě vir; jakýkoliv i situační příznak, že někdo neoprávněně získal osobní údaje - např. spam všem žákům a zákonným zástupcům ve třídě a další.
9.3.	Odpovědný zaměstnanec (garant), je-li to možné, bezodkladně zabrání dalšímu neoprávněnému nakládání, zejména zajistí znepřístupnění, dále vyhodnotí riziko pro práva a svobody fyzických osob, a konzultuje s pověřencem. Pokud ve shodě s pověřencem posoudí jako nepravděpodobné, že by incident měl za následek riziko pro práva a svobody fyzických osob (dále jen „nízké riziko“), provede o incidentu záznam k příslušnému účelu zpracování v komplexním kontrolním záznamu. Pokud vyhodnotí, že nejde jen o nízké riziko, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů nejpozději	Okamžitá změna hesel; zablokování bankovního účtu; sim karty; kontaktování správce systémů k zálohování dat (např. matrika, účetnictví...).

	do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl některý odpovědný zaměstnanec[21] (garant).	
9.4.	Pokud je riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstnanec (garant) vhodným způsobem navíc informuje subjekty údajů[22]. Pokud v konzultaci s pověřencem však vyhodnotí, že již existuje či lze přijmout opatření, díky němuž se vysoké riziko pro subjekty údajů neprojeví, anebo by informování vyžadovalo nepřiměřené úsilí, pouze zveřejní informaci o incidentu na webu školy na výrazném místě.	Např. emailem nebo zveřejněním na webových stránkách.

10. ZÁVĚREČNÁ USTANOVENÍ

	Poznámky a příklady
10.1. Kontrola dodržování směrnice	
10.1.1. Ředitel, případně jeho zástupce zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice pro nakládání s osobními údaji.	Ředitel pravidelně kontroluje zabezpečení a nakládání s osobními údaji a dbá na pravidelné zálohování.
10.1.2. Ředitel, případně jeho zástupce zajistí, aby byly se Směrnicí pro nakládání s osobními údaji seznámeny všechny pověřené osoby.	Seznámení na poradě – podpisy jako doložení seznámení.
10.2. Revize směrnice	
10.2.1. Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.	
10.2.2. Za zpracování, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá ředitel, případně jeho zástupce.	
10.2.3. Revize směrnice se provádí na základě konzultace s pověřencem pro ochranu osobních údajů.	
10.3. Účinnost směrnice	
Směrnice pro nakládání s osobními údaji nabývá platnosti a účinnosti dnem vydání.	26. 9. 2024

V Rakovníku dne 13. 7. 2024

Mgr. Emanuel Vambera

Digitálně podepsal Mgr. Emanuel Vambera
Datum: 2024.09.06 10:48:33 +02'00'

[21] Čl. 33 Obecného nařízení

[22] Čl. 34 Obecného nařízení