\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Základní škola Horšovský Týn, okres Domažlice, příspěvková organizace

**Zámecký park 3, 346 01 Horšovský Týn**

**Vnitřní směrnice GDPR**

O ochraně osobních údajů ZŠ Horšovský Týn

Č. j.: **VD 4 / 2018**

Zpracoval: **Tomáš Roman**

Rozsah působnosti: **Základní škola Horšovský Týn, okres Domažlice, příspěvková organizace**

Účinnost: **1.9.2018**

Počet stran, přílohy:

Originál předpisu je uložen: **u ředitele školy**

Elektronická podoba předpisu: **intranetové stránky školy**

Vydal: **Mgr. Pavel Janský**

Obdrží v tištěné podobě: **zástupci ředitele školy, vedoucí ŠD a ŠJ**

Obsah

[1. Předmět úpravy směrnice 2](#_Toc517945903)

[1.1 Použité zkratky 3](#_Toc517945904)

[2. Definice, pojmy definice oprávněné osoby 3](#_Toc517945905)

[2.1 Vymezení pojmů 3](#_Toc517945906)

[2.2 Oprávněná osoba 4](#_Toc517945907)

[3. Podmínky zapojení zpracovatele 6](#_Toc517945908)

[3.1 Zpracovatel 6](#_Toc517945909)

[3.2 Práva a Povinnosti Správce při spolupráci se Zpracovatelem 6](#_Toc517945910)

[3.3 Seznam Zpracovatelů, popř. kategorie Zpracovatelů pro Organizace 7](#_Toc517945911)

[4. Stanovení účelu zpracování, zpracování OÚ 7](#_Toc517945912)

[5. Informovanost SÚ, souhlasy 8](#_Toc517945913)

[5.1 Vedení evidence souhlasů 10](#_Toc517945914)

[6. Metodika AR, frekvence opakování AR, hodnocení výstupů z AR 11](#_Toc517945915)

[6.1 Metodika analýzy rizik 11](#_Toc517945916)

[6.2 Aktiva 11](#_Toc517945917)

[6.3 Hrozba 11](#_Toc517945918)

[6.4 Zranitelnost 12](#_Toc517945919)

[6.5 Riziko 13](#_Toc517945920)

[6.6 Vypořádání se s riziky 13](#_Toc517945921)

[7. Ochrana osobních údajů 13](#_Toc517945922)

[7.1 Nutnost ochrany OÚ 13](#_Toc517945923)

[7.2 Organizační opatření 14](#_Toc517945924)

[7.3 Řízení přístupů 14](#_Toc517945925)

[7.4 Ochrana osobních údajů v elektronické podobě 15](#_Toc517945926)

[7.5 Ochrana osobních údajů v listinné podobě 15](#_Toc517945927)

[7.6 Bezpečnostní desatero 16](#_Toc517945928)

[8. Formální Posouzení vlivu na ochranu OÚ (DPIA) 17](#_Toc517945929)

[9. Žádosti Subjektů údajů 17](#_Toc517945930)

[9.1 Proces vyřízení žádosti SÚ 18](#_Toc517945931)

[9.2 Typy žádosti SÚ 19](#_Toc517945932)

[9.2.1 Žádost o přístup 19](#_Toc517945933)

[9.2.2 Právo na opravu 19](#_Toc517945934)

[9.2.3 Právo na výmaz (právo být „zapomenut“) 19](#_Toc517945935)

[9.2.4 Právo vznést námitku 20](#_Toc517945936)

[10. Bezpečnostní incidenty 20](#_Toc517945937)

[10.1 Proces a odpovědnost v oblasti řízení incidentů, kategorie incidentů 20](#_Toc517945938)

[10.2 Ohlášení bezpečnostních incidentů 21](#_Toc517945939)

[11. DPO 21](#_Toc517945940)

[11.1 Postavení DPO 21](#_Toc517945941)

[11.2 Informování o DPO 21](#_Toc517945942)

[11.3 Náplň činnosti DPO 22](#_Toc517945943)

[12. Provádění kontroly dodržování opatření 22](#_Toc517945944)

[12.1 Monitorování souladu GDPR 22](#_Toc517945945)

[12.1.1 Audit shody s GDPR 22](#_Toc517945946)

[12.1.2 Kontrola zaměstnanců 22](#_Toc517945947)

[12.1.3 Kontrola bezpečnostních opatření 23](#_Toc517945948)

[12.1.4 Kontrola nastavení přístupů 23](#_Toc517945949)

[12.1.5 IT testování 23](#_Toc517945950)

# Předmět úpravy směrnice

Tato směrnice stanoví základní pravidla a postupy pro zpracování a zabezpečení ochrany osobních údajů fyzických osob v rámci působnosti Základní školy Horšovský Týn, okres Domažlice, příspěvkové organizace, dle **NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES** (dále jako „GDPR“ nebo „Nařízení“). Tato směrnice je závazná pro všechny zaměstnance školy.

## Použité zkratky

|  |  |
| --- | --- |
| OÚ | osobní údaj/e |
| ZKOÚ | Zvláštní kategorie osobních údajů |
| SÚ  | subjekt údajů (vlastník OU) |
| FO | fyzická osoba |
| ICT, IT  | Informační a komunikační technologie |
| IS | Informační systém(y) |
| ÚOOÚ | Úřad pro ochranu osobních údajů (dozorový orgán pro Českou republiku) |
| DPO | Data Protection Officer (pověřenec pro ochranu osobních údajů), jmenovaný, popř. externí |
| GDPR nebo Nařízení  | Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů |
| ORGANIZACE | Základní škola Horšovský Týn, příspěvková organizace |

# Definice, pojmy definice oprávněné osoby

## Vymezení pojmů

Osobní údaj - Osobní údaje jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (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. Osobní údaje jsou jak v elektronické, tak v listinné podobě. Na obě formy se vztahují stejná pravidla zabezpečení.

Zvláštní kategorie osobních údajů (dříve Citlivý údaj) - jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace FO.

Anonymizace, Anonymizovaný osobní údaj – Anonymizovaný osobní údaj je takový údaj, který po provedené úpravě během zpracování (anonymizaci) již nelze vztáhnout k určitému nebo určitelnému subjektu údajů (např. začernění, náhrada osobních údajů jméno, příjmení iniciály apod).

Pseudonymizace - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě. Jedná se o použití „převodní tabulky“, kdy je např. zveřejněna jen tabulka obsahující pořadová čísla SÚ nebo osobní čísla zaměstnanců. Interně je ale k číslům možné přiřadit konkrétní osobu.

Zveřejněný osobní údaj - Zveřejněný osobní údaj je údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Subjekt údajů - Subjektem údajů je FO, jež své osobní údaje vlastní a pro účely zpracování je SÚ Organizaci přímo sděluje nebo je Organizace získává z jiných zdrojů. Subjektem údajů jsou jak zaměstnanci Organizace, tak i třetí osoby (např. dodavatelé, zaměstnanci spolupracujících organizací, představitelé a zaměstnanci orgánů státní správy a územní samosprávy, občané apod.). Subjektem osobních údajů není právnická osoba.

Zpracování osobních údajů - Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení na nosiče informací, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení

WP29 - Pracovní skupina 29 byla ustanovena článkem 29. směrnice 95/46/EC. Jde o nezávislý evropský poradní orgán na ochranu dat a soukromí složený ze zástupců dozorových orgánů. Vydává vodítka a pokyny k jednotlivým tématům GDPR.

## Oprávněná osoba

Oprávněnou osobou pro účely této směrnice se rozumí osoba (zaměstnanec), určená vedoucím úseku Organizace, která v rámci své pracovní činnosti nakládá s osobními údaji, za podmínek a v rozsahu stanoveném vedoucím úseku Organizace. Činnosti zpracování, odpovědnost zaměstnanců a rozdělení kompetencí vychází z Organizačního řádu Organizace.

**Zodpovědnost, kompetence**

|  |  |
| --- | --- |
| Subjekt | Zodpovědnost, kompetence |
| Správce – ředitel organizace | 1. Řízení ochrany osobních údajů – určení a provádění nastavení technických a organizačních opatření ochrany OÚ, ukládání úkolů vedoucím úseků, kontrola plnění opatření
2. Zajištění realizace práv subjektů údajů (výkon realizace DPO)
3. Zodpovědnost za vypracování dokumentace GDPR (tvorba, revize, aktuálnost – Směrnice ochrany OÚ, Záznamy o činnostech zpracování, Evidence souhlasů a žádostí SÚ, Analýza rizik OÚ, Posouzení vlivu DPIA, revize Spisového a archivačního řádu)
4. Zajištění definování účelů, zákonností a prostředků zpracování OÚ pro všechny agendy zpracování OÚ v Organizaci
5. Zajištění školení a seznamování zaměstnanců Organizace s touto směrnicí, Nařízením, povinnostmi při ochraně OÚ a zajištění poskytování informací o procesech souvisejících se zpracováním OÚ
6. Řízení rizik, určení metodiky analýzy rizik, určení aktiv a hrozeb v Analýze rizik OÚ
 |
| Vedoucí úseků | 1. Zodpovědnost za dodržování opatření stanovených touto směrnicí podřízenými zaměstnanci, zejména pak za nezpřístupnění osobních údajů zpracovávaných organizační jednotkou neoprávněným osobám (i v rámci Organizace).
2. Delegování opatření konkrétními pracovními postupy na podřízené zaměstnance
3. Určení oprávněných osob ke zpracování OÚ za svou organizační jednotku pro zpracování OÚ a přiřazení odpovídajících práv = řízení přístupů
4. Stanovení jednotlivých účelů zpracování, stanovení minimálního nutného rozsahu zpracování osobních údajů, stanovení doby uložení osobního údaje a určení zákonnosti podle příslušných agend
5. Seznámení zaměstnanců Organizace s informací o ochraně OÚ, zajištění informovanosti SÚ v oblasti poskytnutí informace a plnění práva na přístup k OÚ
6. Dohlíží na dodržování korektnosti, transparentnosti a minimálního možného zpracování osobních údajů ve vztahu k danému účelu
7. Podávání návrhů opatření a návrhů ke zlepšení procesů při zpracování a ochraně OÚ
8. Spolupracuje s DPO při určení míry dopadu na aktiva a pravděpodobnost hrozby za svou organizační jednotku v Analýze rizik
 |
| Zaměstnanec | 1. Zodpovídá za ochranu každého jednotlivého osobního údaje na svém svěřeném pracovišti a pracovním místě. Je povinen vynaložit veškeré úsilí, aby zabránil vyzrazení, pozměnění nebo ztrátě osobních údajů. A to po celou dobu zpracování nebo uložení osobních údajů na jemu svěřeném úseku.
2. Dodržuje pravidla stanovená touto směrnicí, souvisejícími interními předpisy a legislativou.
3. Neshromažďuje a nezpracovává jiné osobní údaje, než jsou pro daný účel zpracování minimálně nutné, při zpracování jedná maximálně transparentně a korektně
4. ukládá nosiče dat obsahující osobní údaje na náležitě zajištěná místa a při práci s nimi postupuje tak, aby jiná osoba nemohla použít tyto nosiče jako zdroj informací,
5. zachovává mlčenlivost o osobních údajích a o bezpečnostních opatřeních k jejich ochraně. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací,
6. provádí průběžné ničení přípravných podkladů (rukopisů, konceptů, poznámek) sloužících ke zpracování, a to použitím odpovídajících technických a SW prostředků.
 |
| DPO (Pověřenec pro ochranu osobních údajů) | 1. Monitoruje soulad s Nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany osobních údajů a s koncepcemi Organizace v oblasti ochrany osobních údajů
2. Konzultuje a provádí poradenskou činnost zaměstnancům Organizace
3. Vede Záznamy o činnostech zpracování
4. Vypracovává Analýzu rizik, vypočítává míru rizika, připomínkuje katalog aktiv a hrozeb (určení míry dopadu, a pravděpodobnost hrozby ve spolupráci s vedoucími úseků).
5. Zajištění plnění práv SÚ, příprava odpovědí na žádosti SÚ
6. Hlášení porušení zabezpečení povinně ohlašovaných ÚOOÚ/SÚ a evidence bezpečnostních incidentů s vlivem na OÚ/SÚ
7. Spolupracuje, konzultuje a působí jako kontaktní místo pro ÚOOÚ
 |

# Podmínky zapojení zpracovatele

## Zpracovatel

Zpracovatel je jakýkoli externí subjekt, tedy fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatelem se rozumí subjekty, kterým správce systematicky předává OÚ za účelem dalšího zpracování nebo má k dispozici technické a organizační prostředky pro zpracování OÚ (mj. náhled).

Příkladem zpracovatele jsou dodavatelé IS, kteří mají možnost nahlížet do ostrých databází OÚ uložených v IS, příp. ukládat kopie OÚ vzdáleným přístupem na své prostředky, dodavatelé technologií, kdy dochází k ukládání OÚ přímo na prostředky zpracovatele, školitelé, právníci, účetní, marketingové agentury, kterým jsou předávány OÚ za účelem certifikace, tvorby smluv, zpracování mezd apod. Za příjemce OÚ jsou považovány organizace, kterým jsou předávány OÚ v rámci jiné povinnosti (dopravci v rámci plnění smluvního závazku – dodání zboží), předání na základě určení zákonem apod. Správce se stává zpracovatelem, pokud sám neurčil účel a prostředky, ale např. v rámci zpracování navíc zadává OÚ do IS jiného správce.

Za příjemce OÚ se nepovažují Orgány veřejné moci, kterým jsou OÚ sdělovány na základě právní povinnosti pro účely výkonu jejich úředních povinností, jako jsou daňové a celní orgány, finanční vyšetřovací jednotky, nezávislé správní orgány nebo orgány finančního trhu příslušné pro regulaci trhů s cennými papíry a dohled nad nimi, pokud obdrží OÚ, které jsou nezbytné pro provedení konkrétního šetření. Žádost o sdělení OÚ zaslaná orgány veřejné moci by měla být vždy písemná a odůvodněná, měla by se týkat jednotlivého případu a neměla by se vztahovat na celou evidenci ani vést k propojení evidencí.

## Práva a Povinnosti Správce při spolupráci se Zpracovatelem

Za Správce (Organizaci) je pro jednání o vztahu Správce/Zpracovatel **oprávněn jednat ředitel Základní školy Horšovský Týn, příspěvkové organizace.**

Správce (Organizace) je povinen:

1. Subjekty Zpracovatele vybírat obzvláště pečlivě s důrazem na bezpečnost, důvěryhodnost a spolehlivost Zpracovatele. Správce prohlašuje, že vybraní Zpracovatelé poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení a při zpracování byla zajištěna odpovídající ochrana práv SÚ.
2. Uzavřít se Zpracovatelem (nebo se Správcem, pokud je Organizace v pozici Zpracovatele) písemnou smlouvu (dodatek smlouvy), popř. jiný právní akt podle práva Unie nebo členského státu obsahující:
	1. předmět a dobu trvání zpracování,
	2. povahu a účel zpracování,
	3. typ osobních údajů,
	4. kategorie subjektů údajů,
	5. povinnosti a práva správce,
	6. ustanovení, která Zpracovateli ukládají:
		1. zpracování OÚ pouze na základě doložených pokynů Správce
		2. povinnost, aby se osoby Zpracovatele oprávněné zpracovávat OÚ zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
		3. přijmutí opatření minimálně na úrovni zabezpečení zpracování dané touto směrnicí;
		4. dodržování podmínek pro zapojení dalšího Zpracovatele, tedy, že Zpracovatel nezapojí do zpracování žádného dalšího Zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce. V případě obecného písemného povolení Zpracovatel Správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších Zpracovatelů nebo jejich nahrazení, a poskytne tak Správci příležitost vyslovit vůči těmto změnám námitky. Pokud Zpracovatel zapojí dalšího Zpracovatele, aby jménem Správce provedl určité činnosti zpracování, musí být tomuto dalšímu Zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu OÚ, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi Správcem a Zpracovatelem podle bodu 2), a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky Nařízení. Neplní-li uvedený další Zpracovatel své povinnosti v oblasti ochrany OÚ, odpovídá správci za plnění povinností dotčeného dalšího Zpracovatele i nadále plně prvotní Zpracovatel
		5. pokud to vyžaduje povaha zpracování, je Zpracovatel Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv SÚ.
		6. po ukončení poskytování služeb spojených se zpracováním v souladu s rozhodnutím Správce Zpracovatel všechny osobní údaje buď vymaže, nebo je vrátí Správci, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů.
		7. Zpracovatel Správci umožní audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověřil, a k těmto auditům přispěje.

## Seznam Zpracovatelů, popř. kategorie Zpracovatelů pro Organizace

|  |  |
| --- | --- |
| ***Kategorie zpracovatelů (příjemců)*** | ***Konkrétní subjekty*** |
| Dodavatelé IS, hosting, správce IT\* | BAKALÁŘI Software s.r.o., VIS Plzeň, Microsoft |
| Jiné školy, pořadatelé soutěží, pořádající organizace akcí | Sportovní klub Jiskra Domažlice, z. s. – Plavecká škola |
| Dopravci, ubytovací zařízení a poskytovatelé služeb | VIS s.r.o.Plzeň, Earského 14, 326 00 Plzeň |
| Externí školitelé (BOZP, PO, povinné proškolení) | Luboš Sobotka |
| Závodní lékař | MUDr. Luboš Kolář |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

\*dodavatel IS, správce IT nemusí být nutně Zpracovatel. Pokud je jeho servisní zásah jen nahodilým zpracováním OÚ postačí smluvní záruky bezpečnosti a nenakládání s OÚ, ke kterým získá dodavatel (nahodilý) přístup. Vyhodnocení míry přístupu a zpracování OÚ je třeba vždy provádět ve spolupráci IT a DPO.

# Stanovení účelu zpracování, zpracování OÚ

Za stanovení účelu zpracování jsou odpovědní vedoucí úseku, která danou agendu provádí dle Organizačního řádu nebo na základě určení ředitelem školy.

Evidenci účelů zpracování provádí DPO na základě podkladů od vedoucích úseků do Záznamů o činnostech zpracování. Změny v Záznamech o činnostech zpracování dostává ředitel školy na vědomí.

# Informovanost SÚ, souhlasy

Informace je poskytována všem SÚ, jejichž OÚ Organizace zpracovává. Ředitel školy nebo jím pověřená osoba připravuje strukturovanou informaci o zpracování OÚ určenou SÚ, obsah informace konzultuje s DPO.

Informace je připravena pro skupiny SÚ:

1. Zaměstnanci ve formě Informačního memoranda pro zaměstnance
2. Žáci a jejich zákonní zástupci informací ve školním řádu nebo samostatným dokumentem
3. Uchazeči o zaměstnání, návštěvníci školy, akcí školy a webových stránek školy, zástupci spolupracujících organizací na webových stránkách školy nebo jiným vhodným způsobem

Formy poskytování informací (Privacy notice/Zásady zpracování OÚ):

1. Webové stránky Organizace, v patičce každého e-mailu, který odchází z Organizace, je uveden odkaz na webové stránky, část Ochrana Osobních údajů
2. Informační memorandum pro zaměstnance
3. Informace pro zákonné zástupce při zápisu/zahájení školního roku/ve školním řádu – tištěná informace

|  |
| --- |
| Obsah Privacy notice |
| **Poskytnutí informace na základě čl. 13 (při získání OÚ přímo od SÚ)** | **Poskytnutí informace na základě čl. 14 (při získání OÚ jiným způsobem než přímo od SÚ)** |
| a) totožnost a kontaktní údaje správce a jeho případného zástupce**c) účely zpracování, pro které jsou osobní údaje určenyd) právní základ pro zpracování (zákonnost)e) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na zákonném důvodu "oprávněný zájem"**f) případné příjemce nebo kategorie příjemců osobních údajůg) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci***Důležité!******pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) = na SOUHLASU SÚ, je SÚ v informaci vždy upozorněn na existenci práva odvolat kdykoli souhlas, aniž by tím byla dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;******pokud je zpracování založeno na základě*** [***čl. 6***](http://www.privacy-regulation.eu/cs/6.htm) ***odst. 1 písm. f) = OPRÁVNĚNÉM ZÁJMU, včetně profilování založeného na těchto ustanoveních je Subjekt údajů upozorněn na právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají,******V případě podání námitky Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.*** v případě získání údajů od SÚ, v případě potřeby a pro snížení rizika se poskytují dále ještě následující informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:   a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;   b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, jakož i práva na přenositelnost údajů;  d) existence práva podat stížnost u dozorového úřadu;   e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;   f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů. | a) totožnost a kontaktní údaje správce a případně jeho zástupceb) případně kontaktní údaje případného pověřence pro ochranu osobních údajůc) účely zpracování, pro které jsou osobní údaje určenyd) právní základ pro zpracování**e) kategorie dotčených osobních údajů**f) případné příjemce nebo kategorie příjemců osobních údajůg) případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci |

V souladu s určením účelu na jednotlivých úsecích je stanovena i povinnost určit zákonnost daného účelu zpracování. V případě nejasností je možná konzultace právního poradce nebo DPO. V případě, že je zákonnou povinností SOUHLAS se zpracováním OÚ, tedy není možný jiný zákonný důvod a zpracování je i tak nezbytné pro potřeby a naplnění cílů organizace, je třeba **před zahájením zpracování** opatřit souhlasy dotčených SÚ.

1. Souhlas musí být:
	1. Svobodný a odvolatelný
	2. Určitý
	3. Informovaný
	4. Srozumitelný
	5. Jednoznačný
	6. Strukturovaný, tedy pro každou část možnost vyjádření zvlášť
2. Pokud je zpracování založeno na souhlasu, musí být Organizace schopna doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů = vedení evidence souhlasů
3. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.
4. Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.
5. Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.

Souhlas je možné dát písemně nebo službou informační společnosti, případně tzv. konkludentním způsobem, kdy musí být např. návštěvníci akce upozorněni na možnost pořizování fotografií a způsob jejich prezentace např. v pozvánce, na cedulích v areálu, při registraci apod. (navíc oproti standardní Privacy notice informaci). Současně jim musí být poskytnuty informace, že mohou fotografování odmítnout a informace jakým způsobem mohou svůj (konkludentní) souhlas odvolat. Zároveň je vhodné označit fotografa případně oznámit, kdo je oficiální fotograf akce. Organizace musí rovněž po celou dobu zpracování souhlasy evidovat, aby byla schopna udělení souhlasu kdykoliv doložit (v případě konkludentního souhlasu např. dokumentací obsahu a umístění informačních tabulí).

Textaci souhlasu připraví jednotlivé úseky ve spolupráci s DPO, popř. právníkem, za získání souhlasů jsou odpovědní vedoucí úseků, které zpracování (agendu) zajišťují.

Písemné souhlasy jsou vedeny

1. ve spisu, který je veden pro daný účel zpracování spolu s dalšími dokumenty, nebo
2. spolu s dalšími souhlasy potřebnými pro daný účel zpracování

Dokumenty prokazující použití konkludentního souhlasu jsou uchovány v rámci dokumentace konkrétní akce.

Souhlas udělený službou informační společnosti je pouze evidován v evidenci souhlasů.

Odvolání souhlasu mohou SÚ podat na kterémkoliv úseku nebo sekretariátu a to způsobem, jakým souhlas se zpracováním udělily.

**Při odvolání souhlasu je vhodné aplikovat přiměřené ověření totožnosti odvolatele.**

**Posouzení, jaká aktivita je ještě v oprávněném zájmu nebo jiném zákonném důvodu nebo je již třeba vyžádat souhlas subjektů údajů (zákonných zástupců) je velmi citlivá.**

**Řešení:**

**Aktivitám, kterým nelze podřadit legitimitu právní povinnosti, veřejné moci nebo plnění smlouvy, kam lze zařadit hlavní činnosti školy vycházející ze Školského zákona (školní matrika, docházka, vyučování, úrazy, školní jídelna a družina) nebo zaměstnanecké agendy (docházka, zúčtování mezd, SZP, pojištění apod.) je třeba přiřadit jinou legitimitu.**

**Oprávněný zájem:**

**Přiměřená prezentace v rámci prostor školy, historie školy – pořízení fotografií nebo tvorby žáků, diplomů, ocenění, úspěchů za účelem vystavení v prostorách školy včetně uvedení jména, příjmení a třídy, pořízení video/audio záznamu v rámci vyučování pro potřeby rozboru a výuce žáků např. prezentačním dovednostem, vydávání školního časopisu bez distribuce veřejnosti.**

**Souhlas**

**Prezentace mimo prostory školy - pořízení fotografií nebo tvorby žáků, diplomů, ocenění, úspěchů, audiovizuální záznam z vystoupení za účelem vystavení mimo prostory školy, veřejně – např. webové stránky, rajce.net, Facebook a jiné sociální sítě, otištění v časopisech, denících, novinách, kronice, propagačních materiálech distribuovaných veřejně, včetně uvedení jména, příjmení a třídy, souhlas s pořízením třídní skupinové fotografie, resp. její předání ostatním a zpřístupnění na internetu.**

Souhlas návštěvníků akcí pořádaných školou je možné získat konkludentně – viz výše.

## Vedení evidence souhlasů

Ředitel školy vede centrální evidenci souhlasů za všechny organizační jednotky (Organizace). Udělení nebo odvolání souhlasu s konkrétním zpracováním OÚ hlásí všichni zaměstnanci a vedoucí úseků řediteli školy.

# Metodika AR, frekvence opakování AR, hodnocení výstupů z AR

**Analýza rizik se provádí zpravidla 1x za 2 roky**, případně dle potřeby při změně účelů zpracování OÚ (aktiv) nebo změně hrozeb, případně při zavádění nových činností Organizace.

Analýzu rizik (určení dopadů a pravděpodobnost hrozeb) připravuje písemně DPO ve spolupráci s odbornými útvary, zodpovědnost za vedení a aktuálnost řízené interní dokumentace GDPR obecně má správce (ředitel). DPO dále navrhuje opatření ke zmírnění rizik, jejich realizace je pak v kompetenci ředitele a vedoucích úseků ZŠ Horšovský Týn. Organizace provádí Analýzu rizik podle metodiky, viz níže.

DPO pravidelně kontroluje a reviduje aktiva, hrozby a používanou metodiku.

## Metodika analýzy rizik

Postup zpracování analýzy rizik je dán níže uvedeným diagramem a má následující fáze:

1. Identifikace aktiv, posouzení dopadu
2. Určení hrozeb aktivům a jejich ohodnocení
3. Posouzení bezpečnostních opatření a přiřazení hodnoty zranitelnosti
4. Výpočet rizika
5. Návrh dodatečných opatření podle hodnoty rizika

## Aktiva

Hodnota aktiva bude určena pro každý účel zpracování posouzením dopadu, která SÚ hrozí v případě, že by došlo k naplnění hrozby. Hodnotí se:

|  |  |
| --- | --- |
| ***Potenciální újma SÚ*** | ***Vysvětlení*** |
| Reputační škoda | Poškození jména, snížení uplatnění atd. |
| Zneužití identity | Možná krádež identity |
| Obtěžování | Využití třetí stranou pro nevyžádanou nabídku produktů/služeb, využití jako nástroj šikany apod. |
| Ztráta soukromí | Vyzrazení bydliště, telefonního čísla atd. |

Hodnota dopadu se stanoví pro každou ze čtyř možností újmy, která by byla způsobena subjektu OÚ v případě úniku, zneužití, zcizení OÚ (Reputační škoda, Zneužití identity, Obtěžování, Ztráta soukromí). **Hodnotitelem jsou vedoucí úseků za svou organizační jednotku.**

|  |  |  |
| --- | --- | --- |
| 1 | Nízký | Nemá vliv na život subjektu |
| 2 | Střední | Limituje subjekt |
| 3 | Vysoký | Vyžaduje změny chování a jednání subjektu |

Celková hodnota aktiva hodnocením dopadu je vypočtena jako aritmetický průměr z hodnot dopadu pro každou možnost potenciální újmy subjektu údajů:

Hodnota aktiva = Dopad (Reputační škoda \* Zneužití identity \* Obtěžování \* Ztráta soukromí)/4

Výsledná hodnota aktiva nabývá hodnot v krocích po 0,25 od **1,00 do 3,00**.

## Hrozba

Definice hrozby: hrozba je potenciální příčina bezpečnostní události nebo bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.

|  |  |
| --- | --- |
| ***Hrozba*** | ***Popis hrozby*** |
| Lidská chyba - neúmyslná (z nepozornosti, nedbalosti, neznalosti) | K poškození práv a svobod SÚ dojde neúmyslně při činnosti zpracování nebo při podpůrných činnostech. |
| Zneužití OÚ oprávněnými osobami | Dojde ke zneužití informací uložených v listinné nebo elektronické podobě, OÚ jsou použity k jinému než povolenému účelu nebo jiným způsobem než popisuje tato směrnice/legislativa. |
| Neoprávněný přístup, únik informací z nosičů – listinná podoba | OÚ v listinné podobě jsou zpřístupněny osobám, které k tomu nebyly oprávněny (systémová chyba=chybné nastavení přístupu, nahodilá událost=odemčená kancelář, dokumenty na stole jsou přístupné i cizím osobám, jsou zveřejněny seznamy OÚ bez legálního účelu zpracování).  |
| Neoprávněný přístup, únik informací z nosičů – elektronická podoba | OÚ v elektronické podobě jsou zpřístupněny osobám, které k tomu nebyly oprávněny (systémová chyba=chybné nastavení přístupových práv, nahodilá událost=únik přístupových údajů, odeslání seznamu OÚ e-mailem na nesprávnou adresu, zveřejnění OÚ na webových stránkách bez legálního účelu zpracování, zaměstnanec zkopíruje databázi zákazníků na USB flash a prodá jí konkurenci.). |
| Porušení zákonných předpisů | Při zpracování jsou porušeny zásady korektnosti, transparentnosti a bezpečnosti nebo přímé postupy dané legislativou/pracovními postupy. |
| Živelní událost (požár, voda, ostatní) - fyzické poškození nebo zničení OÚ nebo technických nosičů, havárie technických prostředků | Událost, při které dojde ke ztrátě nebo zničení (např. požár, povodeň), havárie technický prostředků. Bez ohledu na formu zpracování (listinná nebo elektronická) |
| Kybernetická hrozba - útok zvenčí | Dos, DDos útok, útok ransomware, šifrování, trojské koně, malware, phishing, tabnabbing apod. |

Hodnotitel hodnotí pravděpodobnost hrozby pro každé aktivum (účel zpracování). **Hodnotitelem jsou vedoucí úseků za svou organizační jednotku.**

Stupnice hodnocení pravděpodobnosti hrozby

|  |  |  |
| --- | --- | --- |
| ***Body*** | ***Pravděpodobnost*** | ***Definice pravděpodobnosti*** |
| 1 | Nízká | Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za rok. |
| 3 | Střední | Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku. |
| 5 | Vysoká | Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je kratší než 1 měsíc. |

## Zranitelnost

Definice zranitelnosti: zranitelností je slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami. **Hodnotitelem jsou vedoucí úseků za svou organizační jednotku.** Hodnotitel určuje míru zranitelnosti na stupnici 1-4:

|  |  |  |
| --- | --- | --- |
| 1 | Nízká | Zranitelnost je málo pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována |
| 2 | Střední | Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost podléhá kontrolním mechanismům. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření. |
| 3 | Vysoká | Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření. |
| 4 | Kritická | Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezená. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření |

## Riziko

Pro každý účel zpracování (aktivum) a hrozbu je stanoveno riziko podle vzorce: **riziko = celková hodnota aktiva x zranitelnost x hrozba. Riziko každého účelu (aktiva) může dosahovat hodnot v rozmezí 1,00 až 60.**

|  |  |  |  |
| --- | --- | --- | --- |
| Stupeň rizika (počet bodů) | Od | Do | Opatření |
| nízká | 1 | 5,99 | Opatření jsou dostatečná |
| střední | 6 | 18,99 | Opatření je třeba revidovat, riziko je možné přijmout (vedoucí odboru) |
| vysoká | 19 | 44,99 | Opatření je třeba neprodleně revidovat, riziko je možné přijmout písemně vedením Organizace |
| kritická | 45 | 60 | Riziko není možné přijmout, je nutné přijmout další opatření, popř. konzultovat s ÚOOÚ |

Výpočet rizika, představení výsledku Analýzy rizik vedení Organizace a návrhy opatření pro snížení rizika provádí DPO.

Cílem hodnocení rizik je:

* prokázat, že navržená bezpečnostní opatření jsou dostatečná,
* identifikovat případnou potřebu realizace dodatečných bezpečnostních opatření.

## Vypořádání se s riziky

Povinností Organizace je projednat výstupy z analýzy rizik a rozhodnout o dalším postupu ve vypořádání rizik, které může být následující:

* akceptace zvýšeného rizika (úroveň střední - vysoká) zejména z důvodu ekonomické neúnosnosti protiopatření;
* akceptaci středních rizik může učinit samostatně i vedoucí odboru s vědomím vedení
* akceptaci vysokých rizik musí rozhodnout porada vedení
* rozhodnutí o vyhnutí se riziku:
	+ neprovádění určitých aktivit (např. může být rozhodnuto, že IS nebude zpracovávat určité údaje nebo bude omezen přístup k nim);
	+ přemístěním aktiv mimo oblast rizika;
* rozhodnutí o přenesení rizika na třetí stranu (dodavatel, pojišťovna, …);
* přeskupení aktiv tak, aby se snížila jejich hodnota (např. rozložení informací na více míst apod.), uvolnění dalších zdrojů pro řešení rizik a přijetí opatření, které eliminuje riziko.

# Ochrana osobních údajů

## Nutnost ochrany OÚ

Osobní údaje jsou vlastnictvím Subjektů údajů, a proto je třeba při jakémkoli zpracování dodržovat nejen pravidla zákonnosti, korektnosti a transparentnosti, ale je nutné je také odpovídajícím způsobem chránit zejména před náhodným nebo protiprávním zničením, ztrátou, pozměňováním, neoprávněným zpřístupněním předávaných, uložených nebo jinak zpracovávaných OÚ, nebo neoprávněný přístup k nim. Riziko škody/újmy SÚ zohledňuje Správce prováděním Analýzy rizik.

Na základě výsledků Analýzy rizik s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování určuje Správce technická a organizační opatření touto směrnicí, aby zajistil úroveň zabezpečení odpovídající danému riziku, zejména pak zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování a schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.

## Organizační opatření

Organizace zajistila obecné proškolení všech zaměstnanců prokazatelným způsobem s GDPR k 25. 5. 2018. Organizace zajistí proškolení v případě změn legislativy a promítnutí legislativních změn do interních předpisů. Školení je zaměřeno zejména na povinnosti organizace, povinnosti zaměstnanců, jejich odpovědnost a principy ochrany osobních údajů.

Vedoucí zaměstnanci dbají na aplikaci principů ochrany osobních údajů a transparentního a korektního zpracování při zpracování OÚ zaměstnanci.

Organizace zajišťuje proškolení nových zaměstnanců s principy GDPR a ochrany osobních údajů prostřednictvím této směrnice. Seznámení se směrnicí a základní informací o zpracování osobních údajů zaměstnanců je součástí úvodního zaškolení zaměstnance.

Organizace zajistí dodatečné odborné školení oprávněných osob na základě zařazení školení do plánu odborných školení, na základě výsledků Analýzy rizik nebo výsledků kontrol nastavených opatření a případně na základě vyhodnocení bezpečnostních incidentů.

Organizace zajišťuje kompetence a procesy pro zajištění informovanosti SÚ, plnění práv SÚ a ochrany OÚ prostřednictvím této směrnice.

Organizace zajišťuje specifická školení v oblasti kybernetické bezpečnosti a trendech v informatice v rámci odborného vzdělávání vedoucích pracovníků a pracovníků IT.

## Řízení přístupů

1. Přístup do aplikace spravující OÚ (Bakaláři, Gordic, Qasar, VIS), přístup k souborům obsahující OÚ uložených na sdílených úložištích a přístup k úložištím listinné dokumentace obsahující OÚ (např. přidělením klíčů, kódů a poučením o nepředávání klíčů nebo přístupových údajů dalším osobám) mají pouze osoby k tomu pověřené.
2. Pověření viz bod 1. uděluje ředitel školy nebo jeho zástupce. To platí pro určení rozsahu oprávnění pro nového zaměstnance i pro změny ve stávajícím rozsahu oprávnění.
3. Přístup k osobním údajům žáků a jejich zákonných zástupců ve školní dokumentaci mohou nahlížet:
	1. 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),
	2. do údajů žáka ve školní matrice
		1. třídní učitel má přístup k údajům žáků a zákonných zástupců jemu přidělené třídy,
		2. ředitel školy, zástupce ředitele, správce počítačové sítě má přístup k celé databázi,
		3. zákonný zástupce má přístup jen k údajům svého dítěte.
	3. do údajů o zdravotním stavu žáka, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv - výchovný poradce, vedoucí pedagogičtí pracovníci, třídní učitel, učitel předmětu, na který má žák nějaké zdravotní omezení
	4. 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.

## Ochrana osobních údajů v elektronické podobě

1. Aplikace (IS) a jednotlivé pracovní stanice provozované Organizací jsou chráněny před působením škodlivého kódu nasazením antivirového systému.
2. Vnitřní síť ORGANIZACE je oddělena od veřejných sítí firewallem. Firewall má povoleny služby a porty nutné pro fungování provozovaných aplikací, vše ostatní je uzavřeno. O otevření portu a služeb rozhoduje ředitel nebo jí pověřená osoba (správce ICT). Firewall musí odolat DoS a DDoS útokům.
3. Firewall vytváří záznamy o útocích, o zdrojích útoků, o akci, která byla firewallem provedena. K záznamům mají přístup správci IT.
4. Přístup k síti ORGANIZACE a jejím zdrojům a k osobním údajům je možný jen na základě úspěšné autentizace do domény. Pro autentizaci je používána kombinace uživatelského jména a hesla. Heslo musí být minimálně 8 znaků dlouhé, musí kombinovat velká a malá písmena, číslice a speciální znaky. Heslo je měněno minimálně 1x za 6 měsíců. Po 3 neúspěšných pokusech je účet zablokován. Odblokovat účet je oprávněn pracovník IT.
5. Na stanicích a mobilních zařízeních je nastaven časový interval, po kterém dojde k zamčení (stanice/displeje). Interval nesmí být kratší než 30minut.
6. Všichni uživatelé jsou při zřízení uživatelských účtů poučení o povinnosti striktního zákazu sdělování přístupových údajů dalším osobám nebo jejich uchování nezabezpečeným způsobem (lístečky na stole, nástěnce, monitoru, na/v telefonu/mobilním zařízení) apod.
7. Doména vytváří záznamy o přihlášení a o neúspěšných pokusech o přihlášení. K záznamům mají přístup pracovníci IT.
8. Data a osobní údaje jsou zálohovány. Zálohování je prováděno zálohovacím systémem, který nastavují pracovníci IT.
9. Uživatelé PC stanic ukládají data primárně přímo v síťové aplikaci nebo na zálohovaná síťová úložiště k tomu určená. Na lokální počítače jsou ukládána zejména data dočasná, pracovní apod. s vědomím, že nedochází k jejich záloze – a tudíž může dojít k jejich ztrátě. Osobní údaje zaměstnanců a citlivé údaje žáků a jejich zákonných zástupců nejsou ukládány na lokální disky nikdy.
10. Uživatelé nesmí používat USB flash zařízení v Organizaci pro uchovávání dat. Výjimkou je krátkodobé uložení dat na USB flash pro přenos dat mezi stanicemi v rámci Organizace.
11. Je zakázáno vynášet na jakémkoli zařízení data Organizace. Výjimku tvoří zaměstnanci s přidělenými služebními notebooky (NTB) a zaměstnanci, kteří mohou pracovat mimo areál Organizace (např. Home office).
12. Data na NTB se primárně neukládají (využití síťových úložišť). Pokud jsou na NTB uloženy osobní údaje, je uložen na oddílu, který je chráněn šifrováním (např. BitLocker).

## Ochrana osobních údajů v listinné podobě

1. Osobní údaje v listinné podobě jsou uchovávány v uzamčených místnostech. Není možné, aby měla k osobním údajům přístup neoprávněná osoba. V pracovní době není možný přístup na jednotlivá pracoviště v nepřítomnosti odpovídajícího pracovníka. Úklid kancelářských prostor je prováděn v pracovní době a za přítomnosti oprávněných osob v kanceláři.
2. 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 zástupce ředitele školy). Třídním učitelům jsou zapůjčeny na nezbytně dlouhou dobu k provedení zápisů. Vyučující jednotlivých předmětů zapisují jen klasifikaci dle svého úvazku. Třídní výkazy, katalogové listy, další materiály ze školní matriky či jejich části nelze vynášet ze školy, předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.
3. V případě návštěvy kanceláře/kabinetu třetí stranou musí být listiny s osobními údaji uloženy takovým způsobem, že třetí strana nebude mít možnost osobní údaje odečíst.
4. Při přenášení listin obsahujících osobní údaje je nutné věnovat této činnosti zvýšenou pozornost tak, aby nedošlo ke ztrátě takových listin nebo zpřístupnění OÚ neoprávněným osobám.
5. V případě, že přeprava dokumentů obsahující osobní údaje je svěřena jiným, k tomu určeným subjektům, je oprávněná osoba povinna tyto dokumenty umístit samostatně podle jednotlivých adresátů v uzavřených obalech (např. zalepená obálka nebo krabice s přelepem a signaturou či razítkem).
6. Dokumenty se zvýšeným rizikem narušení soukromí nebo svobod SÚ nebo s vyšší hodnotou pro Organizaci jsou vždy chráněny dalšími prvky objektové bezpečnosti – umístěním v zamykatelném šuplíku nebo skříni a navíc elektronickým zabezpečovacím zařízením, popř. mřížemi a zvýšenou ochranou proti požáru (EPS).

## Bezpečnostní desatero

ORGANIZACE dbá na bezpečnost osobních údajů, dat a informací. Všechna bezpečnostní opatření a bezpečnostní mechanismy jsou však neúčinné pokud není dodržován elementární bezpečnostní přístup uživatelů informačního systému.

V této souvislosti je níže uvedeno několik **základních pravidel, které je potřeba mít neustále na paměti**.

1. Při jakkoli krátkém opuštění svého pracovního místa je **nutné** zamknout pracovní stanici (zkratka Win+L, odhlášení);
2. Při jakkoli krátkém opuštění svého pracovního místa je třeba **veškeré** materiály, které svým charakterem obsahuji **citlivé informace** (osobní údaje, interní informace, apod.) alespoň uložit do zásuvky – tzv. zásada čistého pracovního stolu; **obzvláště to platí pro ty, kteří přicházejí v kanceláři ke styku s třetími stranami** (rodiče dětí, dodavatelé, uchazeči o zaměstnání atp.);
3. Při pořizování kopií a skenování je potřeba se přesvědčit, zda v kopírce/skeneru nezůstal originál dokumentu;
4. Při tisku dokumentů, které svým charakter odpovídají citlivé informaci, je potřeba si tisk **okamžitě** vyzvednout u tiskárny, a to v případě tisku na sdílené stroje. Je potřeba mít přitom na zřeteli i dokumenty, které se „zaseknou“ v tiskové frontě a mohly by se vytisknout „samy“ později. Stejně tak je potřeba se přesvědčit, zda netisknete náhodou na jinou než zamýšlenou tiskárnu;
5. V případě elektronické komunikace, zkontrolujte adresáta emailu, aby zpráva nebyla omylem odeslána nezamýšlené osobě. Nepřeposílejte obsah komunikace s třetí osobou a pokud to není nutné, nepoužívejte volbu „odpovědět všem“ – Reply to all.
6. **Citlivé informace je povoleno ukládat jen na zabezpečená interní datová uložiště**. Je zakázáno ukládat citlivá a nezabezpečená data (šifrováním nebo dostatečně silným heslem) na cloudová uložiště (DropBox, SkyDrive, uloz.to, uschovna.cz apod.);
7. **Při práci s elektronickou poštou je potřeba být obezřetný** a dostatečně rezistentní vůči emailům s podvodným a potencionálně nebezpečným obsahem. Neotevírat a **neklikat v emailu na odkazy a neotevírat přílohy**, pokud není jistota pravosti obsahu – věrohodný odesilatel, informace v emailu a případně adresy uvedených odkazů. **Nezapomeňte na to, že email je snadné zfalšovat a podvrhnout**;
8. Na prostředcích ORGANIZACE a na všech prostředcích, které jsou připojeny do sítě ORGANIZACE, **není dovoleno** **navštěvovat internetové stránky** s potenciálně nebezpečným obsahem (erotické stránky, „warez“ stránky apod.) a **taktéž z internetu stahovat obsah, který nesouvisí s pracovní činností** (jakýkoliv software). **Svěřené pracovní prostředky nejsou určeny k soukromým účelům**. Uživatelům je zakázáno v IT prostředí Organizace používání vlastních paměťových médií (diskety, CD a DVD, USB paměti, atp.);
9. Je potřeba kontrolovat a zavírat za sebou vstupní dveře, které oddělují veřejně dostupné prostory od interních a **být obezřetný ke komukoli, koho neznáte**. Ti, kteří mají přístup do serveroven a jiných neveřejných prostor, se před odchodem musí přesvědčit, že za sebou nenechali otevřené a nezamčené dveře;
10. Stejně jako čistý stůl je třeba udržovat i pracovní plochu počítače „čistou“. Na plochu patří pouze zástupci často potřebných souborů, složek či aplikací.

# Formální Posouzení vlivu na ochranu OÚ (DPIA)

Povinnost dle čl. 35 GDPR:

*Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek* ***vysoké riziko pro práva a svobody fyzických osob****, provede správce* ***před zpracováním*** *posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.*

DPO spolupracuje s osobou pověřenou zpracováním Posouzení vlivu za Organizaci na vypracování vyhodnocení, jestli je nutné vypracování formálního Posouzení vlivu na soukromí subjektů údajů. DPO má roli poradní, konzultační a metodickou.

Vyhodnocení potřebnosti provedení DPIA je třeba provést vždy, když je do Záznamů o činnostech zpracování přidán nový účel zpracování nebo se výrazným způsobem změní prostředky zpracování stávajícího účelu. O přidání/změně účelu je informován DPO ředitelem školy nebo vedoucím úseku.

Zpracování, ke kterým nebude nikdy třeba formální Posouzení vlivu (DPIA):

**DPIA nebude nikdy provedeno pro agendy, kdy se jedná o činnosti v přenesené působnosti státu.**

ÚOOÚ stanovilo (a seznam se bude rozšiřovat) některé účely, kde DPIA nebude potřeba nikdy (**zpracování při vedení účetnictví, personální a mzdové agendy a sociálního a zdravotního pojištění na základě právní povinnosti**, obchodní činnost včetně newsletterů, věrnostních soutěží a karet – pokud jsou použity pouze běžné osobní údaje, přímý marketing a profilování založeném na výběru a zobrazování položek zboží na webové stránce při jedné návštěvě, **všude tam, kde bylo posouzení vlivu provedeno při přijetí právního předpisu**, zpracování prováděná samostatným lékařem, advokátem nebo notářem nebo poskytovatelem sociálních služeb jako OSVČ a použití kamery ve vozidle za účelem dokumentace nehody a jejímu šetření příslušnými orgány).

Minimální náležitosti posouzení vlivu na ochranu osobních údajů (článek 35, odst. 7):

* + systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;
	+ posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
	+ posouzení rizik pro práva a svobody subjektů údajů
	+ plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob

Provedením posouzení vlivu se reálně posoudí rizika a opatření. Tím, že z vyhodnocení vzešlo zvýšené riziko, je vhodné přidat pro daný účel zpracování opatření ke snížení rizika pro práva a svobody SÚ. V případě, že i po zavedení dodatečného opatření zůstává riziko pro práva osob vysoké, je třeba konzultace s ÚOOÚ.

# Žádosti Subjektů údajů

Žádosti Subjektů údajů mohou mít různou povahu i formu. Žadateli není nikdy odpovídáno bez řádné autentizace Žadatele. Odpověď Žadateli připraví DPO a odešle ředitel.

Žádost o plnění práva SÚ podává žadatel zpravidla:

1. ústně, tj osobní návštěvou Organizace
2. písemně, a to i prostřednictvím sítě nebo služby elektronických komunikací (e-mail podepsaný elektronickým podpisem, datová schránka)

Telefonické žádosti se neevidují a neodpovídá se na ně z důvodu nemožnosti autentizace osoby žadatele. Žadatel je odkázán na písemnou formu žádosti nebo osobní kontakt v Organizaci. U žádostí doručené prostým e-mailem je postupováno stejně, žadatel je odkázán na jinou formu podání z důvodu nemožnosti autentizace SÚ.

**Osobně, telefonicky nebo prostým e-mailem se nikdy nesdělují jakékoliv osobní údaje zaměstnanců žáků a dalších osob osobám, které jsou žadateli o práva subjektů údajů nebo externím subjektům pokud takové předání není podloženo právním důvodem (legalitou).!**

Organizace vyřídí všechny žádosti směřující k plnění práv SÚ podané formou umožňující autentizaci Žadatele. V případě, že ze žádosti není patrné, čeho se žadatel domáhá, bude žádost zamítnuta pro nedůvodnost a žadateli DPO v tomto smyslu odpoví.

Lhůta pro vyřízení žádosti SÚ je 30dnů, v případě, že je třeba delší čas na přípravu, odešle DPO žadateli odpověď ve lhůtě 30dnů od podání v tomto smyslu. Lhůta pro odpověď se může takto prodloužit až o 60 dnů.

## Proces vyřízení žádosti SÚ

1. prvotní reakce na žádost SÚ = kterýkoliv zaměstnanec organizace odkáže Žadatele na ředitele školy, v případě přijetí žádosti v písemné podobě (e-mail, pošta, datová schránka) je žádost evidována ředitelem školy v centrální evidenci žádostí SÚ.
2. přijetí = ředitel školy žádost o plnění práv subjektem údajů posoudí z hlediska formální správnosti – zda je určena organizaci, zda je úplná, tedy je z ní patrné, čeho se žadatel domáhá. V případě ústního podání provede s Žadatelem zápis žádosti, který SÚ potvrdí. Každou relevantní žádost zapíše ředitel školy do centrální evidence žádostí SÚ včetně data podání a kontaktních údajů žadatele.
3. autentizace SÚ= ředitel školy při příjmu žádosti nebo následně prověří, že se jedná o osobu žadatele, resp. osobu oprávněnou za žadatele žádost podat = provede autentizaci osoby žadatele.

Za osobu oprávněnou podat žádost je možné pokládat:

* + - 1. Osobu, jež se při osobním kontaktu prokáže občanským průkazem nebo jinou veřejnou listinou prokazující totožnost.
			2. Podáním žádosti přes datovou schránku osoby, které se žádost týká
			3. Podáním elektronickou poštou v případě podepsání zaručeným elektronickým podpisem (podpis e-mailu, podpis dokumentu žádosti)
			4. Podáním podepsané písemné žádosti doručené Organizaci osobně nebo poštou
1. Ředitel školy předá veškeré relevantní žádosti SÚ včetně kontaktních údajů SÚ a údajů o datu podání žádosti DPO.
2. **DPO ve spolupráci s odbornými útvary zajistí plnění práv SÚ a připraví písemnou odpověď žadateli.** O podrobnosti připravené informace v případě nejasností rozhodne vedoucí úseku, popř. ředitel školy.
3. DPO předá vypracovanou odpověď řediteli školy nejpozději 7 dnů před nejzazším termínem odeslání odpovědi žadateli
4. Ředitel zajistí odeslání podepsané odpovědi nejpozději v poslední den lhůty určené na odpověď:
	1. Žadatel disponuje datovou schránkou = odpověď bude odeslána datovou schránkou.
	2. Žadatel nedisponuje datovou schránkou
		1. žádost byla podána osobně = ředitel školy s žadatelem vyjedná termín osobního převzetí nebo doručení dopisem
		2. žádost byla doručena poštou (i elektronickou) = odpověď bude odeslána poštou.
5. Pracovník podatelny zaznamená data a způsob vyřízení žádosti do centrální evidence žádostí SÚ a uloží případné dokumenty do spisu žádosti.

## Typy žádosti SÚ

### Žádost o přístup

Subjekt údajů má právo získat od Organizace potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím (obsaženy v Příloze č.1 Záznamy o činnostech zpracování v řazení dle účelů zpracování):

- účely zpracování;

- kategorie dotčených osobních údajů;

- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

- plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

- existence práva požadovat od Organizace opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a/nebo vznést námitku proti tomuto zpracování;

- 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, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách podle článku 46, které se vztahují na předání.

Organizace poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může Organizace účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

DPO připraví strukturovanou odpověď na žádost o přístup s obsahem výše uvedených informací, a pokud o to SÚ žádá i kopie dokumentů, které obsahují OÚ žadatele. Při tom nesmí narušit práva a soukromí jiných osob, tedy jiné osobní údaje před odesláním znečitelní. Rozsah poskytnutých kopií určí v každém individuálním případě vedoucí úseku nebo ředitel školy podle typu žadatele.

### Právo na opravu

Subjekt údajů má právo na to, aby Organizace bez zbytečného odkladu opravila nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

Pokud je to možné, DPO zajistí opravu údajů ve všech prostředcích zpracování (osobní spis, datové úložiště, IS)

### Právo na výmaz (právo být „zapomenut“)

Subjekt údajů má právo na to, aby Organizace bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a Organizace má povinnost osobní údaje bez zbytečného odkladu vymazat, **pokud je dán jeden z těchto důvodů**:

- osobní údaje **již nejsou potřebné pro účely, pro které byly shromážděny** nebo jinak zpracovány = vyprší stanovená lhůta pro zpracování (viz Spisová a skartační směrnice);

- **subjekt údajů odvolá souhlas**, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;

- subjekt údajů **vznese námitky proti zpracování (v případě použití zákonného důvodu „oprávněný zájem“)** v případě, že neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování v případě přímého marketingu;

- osobní údaje byly zpracovány protiprávně;

- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na Organizace vztahuje;

- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti v souvislosti přímo dítěti a s jeho souhlasem.

Jestliže Organizace osobní údaje zveřejnila a je povinna je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informovala příjemce a zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

**Organizace při obnově ze zálohy provede kontrolu, zda po obnově nejsou OÚ osob, které byly vymazány, opět aktivní. Kontrolu zajistí metodik ICT po provedení obnovy ze zálohy.**

### Právo vznést námitku

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoliv vznést námitku proti zpracování osobních údajů, které se jej týkají v případě, že je zákonným důvodem oprávněný zájem (GDPR, čl. 6 odst. 1 písmeno f), včetně profilování založeného na těchto ustanoveních. Organizace osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

# Bezpečnostní incidenty

## Proces a odpovědnost v oblasti řízení incidentů, kategorie incidentů

1. Všichni zaměstnanci Organizace jsou povinni hlásit potenciální bezpečnostní událost.
2. V případě, že se jedná o událost vzniklou při elektronickém zpracování dat (práce v IS, elektronické verze dokumentů, e-mail, jiná práce na počítači), hlásí událost přímo řediteli školy, v ostatních případech svému nadřízenému.
3. Ředitel škol nebo správce ICT provedou vyhodnocení události a určí, zdali se jedná o bezpečnostní událost nebo incident. O událost se jedná v případě, že došlo k pouze potenciálnímu vzniku škody (např. antivirový systém identifikoval virovou nákazu), incidentem se rozumí událost, při které již vznikla škoda, nebo je třeba okamžité reakce pro zabránění šíření události a vzniku škody – např. ztráta notebooku).
4. Ředitel školy nebo správce ICT v případě, že vyhodnotí událost jako bezpečnostní incident, provede (příp. ve spolupráci s externím dodavatelem IS) okamžitě opatření, které zamezí dalším škodám.

O incident se jedná v případě, že jde o:

* 1. narušení bezpečnosti informací v IS nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku bezpečnostní události, přičemž v případě porušení dostupnosti a integrity informace se musí jednat o incident, který má dopad na celý IS, modul IS nebo má dopad na více uživatelů. Narušením bezpečnosti rozumíme narušení důvěrnosti, integrity nebo dostupnosti informací, služeb či IS. *Příklad: incidentem je, pokud dojde k zavirování počítače*
	2. krádeže a hlášení ztrát
	3. narušení schválených pravidel v oblasti fyzické bezpečnosti
	4. narušení schválených pravidel v oblasti personální bezpečnosti
	5. narušení schválených pravidel v oblasti administrativní bezpečnosti
	6. narušení schválených pravidel v oblasti bezpečnosti IT
1. Bezpečnostní událost se v Organizaci neeviduje.
2. Bezpečnostní incident správce ICT/ředitel školy nahlásí DPO.
3. DPO vždy eviduje Bezpečnostní incident v evidenci bezpečnostních incidentů.
4. DPO následně posoudí (může si vyžádat dodatečné informace od ohlašovatele), zda:
	1. Se ne/jedná o incident s vlivem na osobní údaje/subjekty údajů
	2. V případě, že se jedná o incident s vlivem na osobní údaje/subjekty údajů posoudí riziko pro práva a svobody FO

**Po identifikaci události je nutné rozhodnout o tom, že se jedná o incident** **s vlivem na osobní údaje/subjekty údajů a o zvýšeném stupni rizika do 72hodin od ohlášení události z důvodu nutnosti ohlášení ÚOOÚ!**

Riziko – při posouzení rizika zařadí DPO incident do tří kategorií:

* + 1. Nízké riziko
		2. Střední riziko
		3. Vysoké riziko

## Ohlášení bezpečnostních incidentů

DPO jako správce evidence bezpečnostních incidentů v případě, že rozhodne o události, že se jedná o incident s vlivem na osobní údaje/subjekty údajů s mírou rizika **střední**, připraví a odešle ÚOOÚ **hlášení o bezpečnostním incidentu**.

V případě, že se bude jednat o incident s vlivem na osobní údaje/subjekty údajů s mírou rizika **vysokou**, připraví a odešle **ÚOOÚ a dotčeným subjektům údajů hlášení o bezpečnostním incidentu**, ledaže by byla splněna kterákoli z těchto podmínek:

1. Organizace zavedla náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování
2. Organizace přijala **následná opatření**, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví
3. Vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Všechny bezpečnostní incidenty hlášené ÚOOÚ se následně projednají na poradě s cílem vyhodnocení a zajištění nápravy, aby se riziko opakování incidentu snížilo.

# DPO

## Postavení DPO

DPO je ve výkonu své role zcela nezávislý na vedení Organizace.

DPO není osobně odpovědný za případy nesouladu s GDPR.

DPO nedostává žádné pokyny týkající se výkonu úkolů v oblasti ochrany osobních údajů od vedení Organizace. To znamená, že při plnění úkolů ochrany osobních údajů nesmí DPO dostávat pokyny jak jednat v dané oblasti, například, jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda konzultovat ÚOOÚ.

Pokud Organizace učiní rozhodnutí neslučitelná s GDPR a s radou DPO, musí mít DPO možnost své nesouhlasné stanovisko vysvětlit těm, kteří tato rozhodnutí udělali.

DPO nesmí být ve střetu zájmů a tak nemůže být nucen vykonávat jiné úkoly a povinnosti, které by k němu vedly.

## Informování o DPO

Ředitel nebo jím pověřená osoba zajistí ustanovení Pověřence pro ochranu osobních údajů (interně, smluvním závazkem) a provede **oznámení kontaktních údajů DPO na ÚOOÚ** a uvedení kontaktních údajů DPO **ve strukturované informaci určené SÚ** (i při každé změně v osobě DPO).

Sdělení kontaktních údajů na DPO vyplývá z povinnosti dle článku 37 odst. 7 GDPR:

* + - 1. dozorovému úřadu, tj. Úřadu pro ochranu osobních údajů.
			2. Veřejnosti – zveřejnění vhodnou formou (např. webové stránky) = Kontaktní údaje DPO jsou zveřejněny tak, aby byly dosažitelné subjektům osobních údajů.

Sdělení kontaktních údajů ÚOOÚ lze učinit podle aktuálních pokynů ÚOOÚ (např. využitím elektronických kontaktů (e-mail: posta@uoou.cz, datová schránka: qkbaa2n) s uvedením předmětu zprávy „oznámení pověřence“.

Obsahem sdělení je:

• identifikace správce nebo zpracovatele, který sděluje kontaktní údaje na pověřence

• označení pověřence (jméno, příjmení)

• kontaktní údaje na pověřence (e-mail, popř. telefon)

## Náplň činnosti DPO

Role DPO vyvíjí činnosti směřující k dodržování ochrany osobních údajů a zajištění výkonu práv subjektů osobních údajů v souladu s požadavky GDPR a to je minimálně:

a) poskytuje Organizaci a jejím zaměstnancům informace a poradenství o jejich povinnostech podle GDPR a dalších předpisů v oblasti ochrany osobních údajů,

b) monitoruje soulad s GDPR, dalšími právními předpisy a vnitřními předpisy a další dokumentací zaměstnavatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců,

c) poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle čl. 35 GDPR,

d) spolupracuje s Úřadem pro ochranu osobních údajů,

e) působí jako kontaktní místo pro Úřad pro ochranu osobních údajů v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl. 36 GDPR, a případně vedení konzultací v jakékoli jiné věci, a

f) působí jako kontaktní osoba zaměstnavatele pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR.

# Provádění kontroly dodržování opatření

Kontrolní činnost a kontrolu provádění bezpečnostních opatření v součinnosti koordinuje DPO v součinnosti s vedoucími pracovníky za každý svěřený úsek (Školní družina, zástupci ředitele pro 1. /2. stupeň, školní jídelna,….):

## Monitorování souladu GDPR

DPO zajišťuje, popř. provádí monitoring souladu s GDPR v oblasti ochrany osobních údajů. Monitoring má podobu pravidelného auditu shody a namátkových kontrol. Z namátkových kontrol a z auditu je zpracován záznam. Výsledek je předkládán vedení Organizace.

### Audit shody s GDPR

Audit se provádí pravidelně 1x ročně, při každé změně rozsahu či kategorií zpracování osobních údajů nebo při změně legislativy s dopadem na ochranu osobních údajů.

Oblasti auditu shody:

* Požadavky GDPR
* Bezpečnostní opatření
* Zpracovatelské smlouvy
* Aktuálnost a úplnost dokumentace

Pravidelné kontroly účinnosti opatření:

### Kontrola zaměstnanců

 - 2 x ročně kontrola organizačního zajištění bezpečnostních opatření – kontrola 2-3 úseků tak, aby každý úsek byl kontrolován alespoň 1x za 2 roky.

Předmět kontroly – organizační opatření – seznámení všech zaměstnanců úseku s touto směrnicí, seznámení se s Privacy notice pro zaměstnance, kontrola existence ustanovení o mlčenlivosti o OÚ v pracovní smlouvě/DPČ/DPP aktuálně platného znění.

### Kontrola bezpečnostních opatření

U všech zaměstnanců kontrolovaného úseku na místě kontrola fyzického zabezpečení dokumentů v listinné podobě (uložení dokumentů, přítomnost na pracovišti, zamykání, prostor pracovní plochy), zamčení pracovní plochy počítače, kontrola ukládání dokumentů v elektronické podobě, ujištění o tvorbě záloh (spolupráce s IT)

### Kontrola nastavení přístupů

Pracovník IT provede 1x ročně kontrolu nastavení přístupů 10 náhodně vybraných uživatelů (plán nastavení přístupů vs. realita), nastavení firewall, nastavení blokování aplikací/webů

### IT testování

Nejméně 1x za 2 roky zajistí pracovník IT:

1. test obnovy ze zálohy
2. penetrační test
3. phishing test