Základní škola Orlová – Lutyně Ke Studánce 1050 okres Karviná, příspěvková organizace

SMĚRNICE č. 6/2018

o nakládání s osobními údaji

Zpracoval:	Mgr. Milan Fus, ředitel školy	Podpis:
Schválil:	Mgr. Milan Fus, ředitel školy	Podpis:
Platnost od:/účinnost od:	24. 04. 2018	25. 05. 2018
Ruší se:	-	
Počet stran:	30	
Počet příloh:	1	
Zrušeno dne:		

Článek 1

Úvodní ustanovení

Tato Směrnice o nakládání s osobními údaji (dále jen tato směrnice a/nebo směrnice) se vydává na základě a v souladu s ust. § 30 odst. 1) zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání, v platném znění (dále jen školský zákon) a v souladu s ust. zákona č. 110/2019 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění.

Systém ochrany osobních údajů definovaný touto směrnicí je navržen a zpracován v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), někdy také General Data Protection Regulation (dále jen Nařízení GDPR nebo Nařízení).

Se směrnicí musí být seznámeni všichni zaměstnanci. Směrnice je všem jejím zaměstnancům přístupná na síťovém disku Pythia/ucitele (v digitální podobě) a v kanceláři ředitele školy (v tištěné podobě). Směrnice se vztahuje i na zaměstnance, kteří pro organizaci pracují na základě dohod o pracích konaných mimo pracovní poměr.

Článek 2

Předmět, účel a působnost

1) Směrnice stanovuje taková opatření a pravidla, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných Základní školou Orlová – Lutyně Ke Studánce 1050 okres Karviná (dále jen organizace). Ochranou osobních údajů je míněno zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich integrity, dostupnosti a dalších bezpečnostních aspektů všech osobních údajů v míře potřebné pro činnost organizace, a to v souladu s Nařízením a jinými právními předpisy.

2) Tato směrnice se zabývá ochranou všech osobních údajů ve vlastnictví nebo ve správě organizace, bez ohledu na jejich podobu (tištěnou, psanou, uloženou elektronicky, odesílanou poštou, předávanou elektronicky, ústním podáním, telefonem, faxem apod.).

3) Za účelem ochrany osobních údajů je v rámci organizace definován tzv. systém řízení ochrany osobních údajů, fungující v souladu s touto směrnicí a těmito dokumenty:

- Organizační řád,
- Spisový řád a skartační plán,

4) Přehled spravovaných datových sad osobních údajů formou Záznamů o činnostech zpracování je zaměstnancům k dispozici na síťovém disku Pythia /ucitele (v digitální podobě) a v kanceláři ředitele školy (v tištěné podobě). Zpracování Záznamů o činnostech zpracování bylo provedeno dialogem s odpovědnými pracovníky organizace. Záznamy o činnostech zpracování jsou pravidelně aktualizovány.

5) Směrnice je závazná pro všechny osoby zařazené do organizační struktury a osoby, které osobní údaje zpracovávají na základě smlouvy uzavřené s organizací jakožto správcem osobních údajů; toto ustanovení musí být součástí obsahu uzavřené smlouvy.

Článek 3

Pojmy a definice

Pro účely této směrnice se rozumí:

1) „**osobními údaji**“ 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;

2) „**zvláštními kategoriemi osobních údajů**“ osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

3) „**biometrickými údaji**“ osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

4) „**zpracováním**“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny 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;

5) „**omezením zpracování**“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

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

7) „**anonymizací**“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů a subjekt údajů není nebo již přestal být identifikovatelným;

8) „**evidencí**“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

9) „**správcem**“ organizace jako orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;

10) „**zpracovatelem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

11) „**příjemcem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty;

12) „**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;

13) „**porušením zabezpečení osobních údajů**“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

14) „**údaji o zdravotním stavu**“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

15) „**záznamem o činnostech zpracování**“ záznamy vedené organizací o zpracování osobních údajů. Záznamy obsahují jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů;

16) „**dozorovým úřadem**“ Úřad pro ochranu osobních údajů;

17) „**Unií**“ Evropská unie;

18) **„Členské státy“** Členské státy Evropské unie.

Článek 4

Rozsah působnosti

1) Vedení organizace (ředitel a zástupce ředitele) odpovídají za to, že pravidla ochrany osobních údajů budou dodržovat zaměstnanci, kteří nakládají s osobními údaji a vystupují v roli uživatelů nebo správců osobních údajů.

2) Pravidla ochrany osobních údajů se vztahují rovněž na všechny další subjekty, které pracují s osobními údaji organizace. Tyto subjekty musí být k dodržování zásad ochrany osobních údajů zavázány postupem dle článku 24 této směrnice.

Článek 5

Určení rolí v systému ochrany osobních údajů

1) Ředitel

Odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nese ředitel zejména:

- schvaluje Směrnici o nakládání s osobními údaji a její aktualizace,
- vyjadřuje se k osobě, která má vykonávat funkci Pověřence pro ochranu osobních údajů (dále také „Pověřenec“),
- jmenuje Pověřence pro ochranu osobních údajů,
- projednává pravidelnou zprávu o stavu ochrany osobních údajů,
- rozhoduje o přijetí technických, fyzických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR.

2) Pověřenec pro ochranu osobních údajů

Pověřenec je jmenován ředitelem a představuje konkrétní osobu zodpovědnou za plnění těchto úkolů:

- poskytování informací a poradenství vedoucím pracovníkům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
- monitorování souladu s touto směrnicí, Nařízením GDPR a dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s vnitřními předpisy organizace v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
- vedení centrální evidence zpracování osobních údajů a její pravidelnou aktualizaci;
- vedení centrální evidence udělených souhlasů se zpracováním osobních údajů;

- zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji;
- zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci v rámci organizace;
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR;
- spolupráce s dozorovým úřadem;
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci.
- působení jako kontaktní místo pro subjekty údajů. Subjekty údajů se mohou obracet na Pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Nařízení.

Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Pověřenec pro ochranu osobních údajů nedostává žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen řediteli. Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí, a to v souladu s právem Unie nebo zákony a právními předpisy České republiky. Pověřenec může plnit i jiné úkoly a povinnosti, které však nesmějí vést ke střetu zájmů jeho činností.

3) Zodpovědné osoby

Ke každé datové sadě osobních údajů je určena Zodpovědná osoba (Zodpovědné osoby jsou uvedeny v Záznamech o činnosti zpracování osobních údajů, které jsou zaměstnancům k dispozici na na síťovém disku Pythia /ucitele (v digitální podobě) a v kanceláři ředitele školy (v tištěné podobě) . Každá Zodpovědná osoba má právo podat Pověřenci návrh na změnu této směrnice, Záznamu o činnostech zpracování, Posouzení vlivu nebo zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice.

Zodpovědné osoby mají právo a zároveň povinnost:

- pro případy vzniku nových druhů osobních údajů tuto skutečnost co nejdříve nahlásit Pověřenci, který provede aktualizaci Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
- informovat bezodkladně Pověřence o všech skutečnostech, které mají vliv na aktuálnost Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
- zabezpečit získání souhlasu subjektu údajů, a to v souladu se zákonem, není-li zpracování možné bez tohoto souhlasu;

- zajistit, aby každý zaměstnanec před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen a proškolen se zásadami ochrany osobních údajů a touto směrnicí a zajistit v roční frekvenci prokazatelné opakování tohoto proškolení;
- zajistit, aby každý zaměstnanec před prvním přístupem ke spravovaným osobním údajům písemně potvrdil Prohlášení o ochraně osobních údajů;
- při uzavírání smluv s třetími stranami dbát na to, aby obsahovaly zásady zajištění ochrany osobních údajů, pokud je to vzhledem k povaze obsahu smlouvy relevantní.

4) Uživatelé osobních údajů

Uživatelem osobních údajů je zaměstnanec používající spravované osobní údaje k plnění svých pracovních povinností. Všichni Uživatelé osobních údajů mají za povinnost:

- dodržovat zásady vyplývající z této směrnice a související dokumentace;
- hlásit veškeré bezpečnostní incidenty svému nadřízenému, případně přímo Pověřenci;
- informovat Pověřence o zjištěných bezpečnostních slabinách;
- informovat Pověřence o změnách ve způsobu zpracování a nakládání s osobními údaji;
- spolupracovat na naplnění práv subjektů údajů;
- vykonávat další činnosti vyplývající z platných vnitřních předpisů organizace, především zajistit průběh skartačního řízení v souladu se Spisovým a skartačním řádem.

5) Správci (Administrátoři)

Správci jsou zaměstnanci, kteří mají na starost provoz a údržbu systémů a aplikací, archivaci a zabezpečení (elektronických) dat uživatelů, a pracovníci odpovědní za řízení a implementaci bezpečnosti systémů. Tito zaměstnanci mají obvykle přístup ke všem datům uloženým v informačním systému nebo fyzický přístup k zařízením, pomocí nichž jsou tato data zpracovávána.

Správci zabezpečují spolupráci s jednotlivými uživateli osobních údajů při ochraně osobních údajů uložených v osobních počítačích, včetně těch přenosných.

Článek 6

Přístup k osobním údajům

1) K osobním údajům mají přístup pouze Zodpovědné osoby, Uživatelé osobních údajů a Správci (Administrátoři).

Článek 7

Zásady zpracování osobních údajů

1) Osobní údaje musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 Nařízení GDPR nepovažuje za neslučitelné s původními účely („účelové omezení“);

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);

d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 Nařízení GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných Nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“).

2) Standardně jsou zpracovávány pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Spis vedený Uživatelem osobních údajů obsahuje pouze informace relevantní pro průběh řízení a agendu s ohledem na minimalizaci údajů k dosažení účelu zpracování.

3) Písemnosti obsahující osobní údaje podléhají procesu fyzické a elektronické skartace v souladu se Spisovým a skartačním řádem, a to včetně dokumentace na vědomí, kopie písemností a dalších dokumentů bez čísla jednacího.

4) Pro statistické účely je nutné osobní údaje anonymizovat.

5) Je třeba zamezit neoprávněnému přístupu ke shromážděným údajům.

Článek 8

Zákonnost zpracování osobních údajů

1) Organizace jako správce osobních údajů zpracovává pouze takové osobní údaje, jejichž zpracování je zákonné. Zpracování osobních údajů je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na organizaci jako správce osobních údajů;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je organizace jako správce osobních údajů pověřena;

f) zpracování je nezbytné pro účely oprávněných zájmů organizace jako správce osobních údajů či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. Toto se netýká zpracování prováděného organizací jako správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.

2) Účel zpracování osobních údajů musí vycházet z výše uvedených právních základů. Osobní údaje nesmějí být použity k jinému účelu, než ke kterému byly pořízeny nebo musí být takové zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je organizace jako správce osobních údajů pověřena.

3) Pokud je zpracování založeno na souhlasu, musí být Uživatel osobních údajů schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.

a) Souhlas musí být udělen samostatně a musí být jasně odlišitelný od ostatních sdělení (jako samostatný dokument). Vzor souhlasu se zpracováním osobních údajů je zaměstnancům k dispozici na síťovém disku Pythia /ucitele (v digitální podobě) a v kanceláři ředitele školy (v tištěné podobě) .

b) Subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu, včetně informace o způsobu odvolání uděleného souhlasu.

c) V případě využití konkludentního souhlasu je nutné zajistit informování subjektu údajů (Informační memorandum na webových stránkách, informační tabule u vstupu na akce, informace na přihlášce, pozvánce, na webovém formuláři a dalších místech sběru osobních údajů).

d) Pro zpracování zvláštních kategorií osobních údajů (biometrické údaje, fotografie, audio, video, zdravotní stav, sociální postavení a další) je nutné vždy udělit samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).

e) Pro zpracování souhlasů s vytvořením kopie občanského průkazu (souhlas podle ust. § 15a zákona č. 328/1999 Sb., o občanských průkazech, v platném znění) je nutné vždy udělit samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).

f) 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 dostupné jako jej poskytnout.

g) Uživatel osobních údajů je povinen ve spolupráci se Správcem (Administrátorem) zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat.

h) Uživatel osobních údajů je povinen vést evidenci datových sad, jejichž zpracování je podloženo uděleným souhlasem subjektu údajů.

4) Zpracování údajů na základě uděleného souhlasu subjektu údajů je využíváno pouze v krajních případech, kdy je zpracování nezbytné a neexistuje jiné oprávnění pro nakládání s osobními údaji.

Článek 9

Opatření pro ochranu osobních údajů

1) Uživatel osobních údajů je povinen dodržovat pravidlo čistého stolu (neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole, po ukončení pracovního dne je každý zaměstnanec povinen takové listinné písemnosti uložit do uzamykatelných úložných prostor a klíče zajistit tak, aby k nim neměly přístup osoby bez oprávnění).

2) Uživatel osobních údajů je povinen v případě odchodu z kanceláře, ve které se již nenachází žádný další zaměstnanec, zavřít okna a tuto místnost zamknout.

3) Uživatel osobních údajů je povinen v případě přítomnosti cizí osoby v kanceláři a nutnosti odchodu zaměstnance z kanceláře, ve které se již nenachází žádný další zaměstnanec, vyprovodit cizí osobu na chodbu, kancelář zamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu zaměstnance do kanceláře (neponechávat cizí osoby bez dozoru v kanceláři).

4) Uživatel osobních údajů je povinen aktivovat spořič obrazovky chráněný heslem kdykoli se vzdálí od pracovní stanice.

5) Uživatel osobních údajů je povinen využívat pro elektronické zpracování osobních údajů k tomu určené informační systémy. Užívání pevných disků pro ukládání písemností obsahujících osobní údaje je povoleno pouze v případě, že není možné tuto dokumentaci ukládat do informačních systémů. Uživatel osobních údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat skartační znaky dle platného Spisového a skartačního řádu.

6) Uživatel osobních údajů je povinen udržovat písemnosti obsahující osobní údaje uložené na pevných discích a ve svých emailových schránkách v souladu s lhůtami stanovenými pro zpracování dle Spisového a skartačního řádu a v minimálním rozsahu umožňujícím dosažení účelu zpracování.

7) Uživatel osobních údajů není oprávněn ukládat písemnosti obsahující osobní údaje na sdílené disky organizace.

8) Uživatel osobních údajů je povinen využívat pro ukládání fyzické dokumentace obsahující osobní údaje (včetně fyzických nosičů elektronické dokumentace) k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění kanceláře uzamknout. Uživatel osobních

údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat skartační znaky dle platného Spisového a skartačního řádu. To platí i pro písemnosti na vědomí, kopie písemností a další dokumenty bez čísla jednacího.

9) Pokud není fyzická dokumentace obsahující osobní údaje uchovávána v uzamykatelných úložných prostorech, musí být zajištěn přístup pouze pro oprávněné zaměstnance (např. úklid pouze s doprovodem oprávněného zaměstnance).

10) Uživatel osobních údajů je povinen udržovat v tajnosti svá přístupová oprávnění (přihlašovací jméno a heslo) k informačním systémům, tato přístupová oprávnění si nezapisovat (na papír, do souboru, apod.) ani je neprozrazovat žádné další osobě.

11) Uživatel osobních údajů je povinen při tisku písemností obsahujících osobní údaje tyto nikdy neponechávat bez dozoru na tiskárně.

12) Uživatel osobních údajů není oprávněn přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé emailové schránky (např. www.seznam.cz, www.gmail.com apod.).

13) Uživatel osobních údajů není oprávněn ukládat na veřejné servery Internetu (např. www.uloz.to, www.uschovna.cz apod.) jakékoli písemnosti obsahující osobní údaje.

14) Uživatel osobních údajů není oprávněn provádět na svěřených prostředcích jakékoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software.

15) Uživatel osobních údajů je oprávněn využívat mobilní zařízení organizace (mobilní telefon, notebook apod.) pouze při dodržení pravidel pro jejich zabezpečení definovaných Správci (Administrátory).

16) Uživateli osobních údajů je umožněno využívat k přístupu k informačním systémům a datům organizace soukromá mobilní zařízení (mobilní telefon, notebook apod.) pouze při dodržení pravidel pro jejich zabezpečení definovaných Správci (Administrátory).

17) Uživatel osobních údajů není oprávněn jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.) na svěřených prostředcích.

18) Uživatel osobních údajů není oprávněn ukládat na vyměnitelná média jakékoliv písemnosti obsahující osobní údaje (mimo jednorázově schválených výjimek). Vyměnitelnými médii rozumíme CD/DVD disky, přepisovatelné CD/DVD, pevné počítačové disky externí, flash disky apod.

19) Každý zaměstnanec, který přichází do styku s písemnostmi obsahujícími osobní údaje uloženými na médiích (CD, DVD, papírové dokumenty, flash paměťové moduly) je povinen zajistit jejich bezpečnou likvidaci (skartování, vymazání, fyzické zničení) v souladu se Spisovým a skartačním řádem.

20) Klíče od kanceláří jsou zaměstnancům vydávány prokazatelným způsobem a je vedena evidence vydaných klíčů. Je zajištěno ukládání a zabezpečení náhradních klíčů od kanceláří a úložných prostor.

Článek 10

Předávání osobních údajů

1) Dokumentaci obsahující osobní údaje v elektronické podobě je povoleno předávat příjemcům mimo organizaci pouze prostřednictvím datových schránek. V případech, kdy není možné dokumentaci předat prostřednictvím datové schránky nebo ve fyzické podobě, lze dokumentaci předat v podobě šifrovaného souboru (např. zip).

Článek 11

Zveřejňování osobních údajů

1) Při zveřejňování osobních údajů musí dojít k opatřením, kdy veškerá zveřejňovaná dokumentace (text, audio, video) bude anonymizována v rozsahu zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění uloženého legislativou (dokumentaci anonymizovat vždy, pokud zákon neukládá jinak).

2) Musí dojít k zajištění anonymizace osobních údajů uvedených v uzavřených smlouvách, které jsou zveřejněny na profilu zadavatele (organizace).

3) Při pořizování jakýchkoliv záznamů z akcí pořádaných v prostorách organizace zajistit informování účastníků o pořizování této dokumentace a uvedení účelu tohoto pořízení.

4) V případě pořizování fotografické nebo video dokumentace z veřejných akcí, musí organizace zajistit informování účastníků o pořizování této dokumentace za účelem zveřejnění na webových stránkách, v kronikách, ve výročních zprávách apod. Pracovníci pořizující tuto dokumentaci musí být viditelně a výrazně označeni.

5) Fotografie zaměstnanců se mohou zveřejňovat na webových stránkách, facebookovém profilu apod., pouze po výslovném souhlasu zaměstnance s tímto zveřejněním (souhlas není vynutitelný). Zveřejnění fotografií zaměstnanců bez výslovného souhlasu je možné pouze u osob, u kterých je to odůvodnitelné (např. vedení organizace).

Článek 12

Získávání informací od subjektu údajů

1) Odpovědný zaměstnanec (Uživatel osobních údajů) v okamžiku získání osobních údajů poskytne subjektu údajů tyto informace:

a) totožnost a kontaktní údaje organizace a jeho odpovědného zaměstnance (Uživatele osobních údajů);
b) kontaktní údaje Pověřence;
c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro jejich zpracování;
d) oprávněné zájmy organizace nebo třetí strany v případě, že je zpracování založeno na opodstatněném zájmu organizace jako správce osobních údajů;
e) případné příjemce nebo kategorie příjemců osobních údajů;
f) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
g) existence práva požadovat od organizace jako správce osobních údajů přístup k osobním údajům týkajících se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
h) existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (pokud je zpracování založeno na uděleném souhlasu se zpracováním osobních údajů);
i) existence práva podat stížnost u dozorového úřadu;
j) 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 poučení ohledně možných důsledků neposkytnutí těchto údajů.

2) Naplnění informační povinnosti podle bodu 1) může být zajištěno zveřejněním Prohlášení o ochraně osobních údajů na webových stránkách.

3) Pokud organizace jako správce osobních údajů hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace v rozsahu dle tohoto článku.

Článek 13

Práva subjektu údajů

1) Subjekt údajů může uplatnit tato práva na:

   a) přístup k osobním údajům
   b) opravu a výmaz osobních údajů
   c) omezení zpracování osobních údajů
   d) přenositelnost osobních údajů
   e) vznesení námitky

2) Naplnění práv subjektů údajů zajišťuje věcně příslušný Uživatel osobních údajů.

3) Způsob podání žádosti o naplnění práv subjektů údajů je zveřejněn na webových stránkách, případně dalšími vhodnými způsoby.

4) Subjektu údajů jsou poskytovány informace v souladu se zásadami zpracování osobních údajů dle čl. 7 této směrnice a to především stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené dítěti.

5) Informace jsou subjektu údajů poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (občanský průkaz, datová schránka).

6) Informace jsou subjektu údajů poskytovány písemně nebo jinou formou, připuštěna je ve vhodných případech i elektronická forma. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty pouze ústně.

7) Informace jsou subjektu údajů poskytovány bez zbytečného odkladu a v každém případě ve lhůtě do jednoho kalendářního měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další maximálně dva kalendářní měsíce, kdy subjekt údajů musí být o takovém odůvodněném prodloužení lhůty k poskytnutí údajů informován nejpozději ve lhůtě do jednoho kalendářního měsíce od obdržení žádosti.

8) Pokud opatření, o něž subjekt údajů požádal, nejsou přijata, musí být subjekt údajů bezodkladně a nejpozději ve lhůtě do jednoho kalendářního měsíce od přijetí žádosti informován o důvodech nepřijetí opatření a o jeho možnosti podat stížnost u dozorového úřadu a o možnosti žádat o soudní ochranu.

9) Poskytované informace, veškerá sdělení a veškeré úkony se poskytují a činí bezplatně. Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, lze přistoupit k:

a) uložení přiměřeného poplatku zohledňujícího administrativní náklady spojené s poskytnutím požadovaných informací, sdělení, anebo s učiněním požadovaných úkonů;

b) odmítnutí žádosti vyhovět.

Zjevnou nedůvodnost nebo nepřiměřenost žádosti je nutné odůvodnit a zdokumentovat pro potřebu následného doložení.

10) Pravidla naplnění práv subjektů údajů jsou uvedena v příloze této Směrnice.

Článek 14

Právo subjektu údajů na přístup k osobním údajům

1) Subjekt údajů má právo získat od organizace jako správce osobních údajů 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:

a) účely zpracování;

b) kategorie dotčených osobních údajů;

c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;

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

e) existence práva požadovat od organizace jako správce osobních údajů opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

2) Organizace jako správce osobních údajů poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může organizace jako správce osobních údajů 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.

3) Právem získat kopii uvedenou v předchozím odstavci nesmějí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Článek 15

Oprava a výmaz osobních údajů

1) Subjekt údajů má právo na to, aby organizace jako správce osobních údajů 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.

2) Subjekt údajů má právo na to, aby organizace jako správce osobních údajů bez zbytečného odkladu vymazala osobní údaje, které se daného subjektu údajů týkají, a organizace má povinnost osobní údaje bez zbytečného odkladu vymazat (tzv. „právo být zapomenut“), pokud je dán jeden z těchto důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování a jejich uchovávání;
c) subjekt údajů vznese námitky proti zpracování s ohledem na uplynutí lhůty pro zpracování nebo s ohledem na prokazatelnou nedostatečnost zabezpečení osobních údajů;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být skartovány ke splnění právní povinnosti stanovené právem Unie nebo zákony a platnými právními předpisy České republiky, které se na organizaci jako správce osobních údajů vztahují.

3) Jestliže organizace jako správce osobních údajů osobní údaje zveřejnila a je povinna je podle odstavce 2 vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně všech technických opatření, aby informoval zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

4) Odstavce 2 a 3 se neuplatní, pokud je zpracování nezbytné:

a) pro výkon práva na svobodu projevu a informace;
b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo ČR, které se na organizace jako správce osobních údajů vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je organizace pověřena;
c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 Nařízení GDPR;
d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle zvláštních právních předpisů;
e) pro určení, výkon nebo obhajobu právních nároků.

Požadavek subjektu údajů na výmaz tedy nelze splnit, pokud je zpracování nezbytné pro splnění právní povinnosti.

Článek 16

Právo na omezení zpracování

1) Subjekt údajů má právo na to, aby organizace jako správce osobních údajů omezila zpracování, v kterémkoli z těchto případů:

a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby organizace jako správce osobních údajů mohla přesnost osobních údajů ověřit;

b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;

c) organizace jako správce osobních údajů již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;

d) subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody organizace jako správce osobních údajů převažují nad oprávněnými důvody subjektu údajů.

2) Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.

3) Subjekt údajů, který dosáhl omezení zpracování, musí být předem upozorněn na to, že bude omezení zpracování zrušeno.

Článek 17

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

1) Organizace jako správce osobních údajů je povinna oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré provedené opravy nebo výmazy osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Organizace jako správce osobních údajů informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.

2) Naplnění informační povinnosti podle bodu 1) může být zajištěno zveřejněním Prohlášení o ochraně osobních údajů na webových stránkách.

Článek 18

Právo na přenositelnost údajů

1) Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl organizaci jako správci osobních údajů, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu organizace jako správce osobních údajů bránila, a to v případě, že:

a) zpracování je založeno na uděleném souhlasu se zpracováním osobních údajů nebo na uzavřené smlouvě; a;

b) zpracování se provádí v elektronické podobě.

2) Subjekt údajů má právo na to, aby osobní údaje předala přímo organizace jako správce osobních údajů druhému správci, je-li to technicky proveditelné.

3) Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je organizace jako správce osobních údajů pověřena.

4) Uplatněním práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Článek 19

Právo vznést námitku

1) Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají. Organizace jako správce osobních údajů 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.

2) Subjekt údajů je na právo vznést námitku výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

Článek 20

Řešení případů porušení zabezpečení osobních údajů

1) Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec neprodleně svému nadřízenému nebo přímo Pověřenci pro ochranu osobních údajů.

2) Okamžité hlášení bude obsahovat minimálně tyto informace:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů pro organizaci jako správce osobních údajů a pro subjekty údajů;

c) návrh okamžitých opatření k zastavení porušení zabezpečení osobních údajů a případně návrh okamžitých nápravných opatření.

3) Pověřenec pro ochranu osobních údajů ve spolupráci se Zodpovědnou osobou, Uživateli osobních údajů, Správci (Administrátory), relevantními zpracovateli osobních údajů, případně dalšími relevantními zaměstnanci, rozhodne o dalším postupu.

4) Pověřenec pro ochranu osobních údajů neprodleně informuje ředitele a předloží mu ke schválení návrh na řešení případu porušení zabezpečení osobních údajů a případně doporučení ohlášení porušení zabezpečení osobních údajů dozorovému úřadu.

5) Pověřenec pro ochranu osobních údajů neprodleně předloží řediteli ke schválení návrh nápravných opatření pro zamezení opakování obdobného porušení zabezpečení osobních údajů. Nápravné opatření obsahuje kroky obnovy a postup, jak zamezit opakování stejného porušení zabezpečení, termíny realizace opatření, jména zaměstnanců odpovědných za jejich splnění. Návrh nápravných opatření musí být konzultován s relevantními Zodpovědnými osobami, které ho svým podpisem odsouhlasí. Realizace nápravných opatření podléhá schválení ředitelem.

6) Pověřenec pro ochranu osobních údajů provádí kontrolu plnění nápravných opatření a výsledky předkládá řediteli v termínech k tomu dohodnutých.

Článek 21

Činnost při zjištění porušení zabezpečení osobních údajů

1) Jakékoli porušení zabezpečení osobních údajů nebo ztrátu dostupnosti osobních údajů (dále jen incident) nebo podezření na takové porušení je každý povinen hlásit řediteli.

2) Podezření na incident se posuzuje pro potřeby postupu podle této směrnice stejně jako incident, dokud není zjištěno, že incident nevznikl.

3) Ředitel je odpovědný za řízení reakce na incident.

4) Ředitel oznámí neprodleně incident nebo podezření na incident Pověřenci pro ochranu osobních údajů a projedná s ním případnou součinnost a komunikaci.

5) Ředitel spolupracuje při řízení reakce na incident s uživateli osobních údajů a pokud je potřebné nebo nutné, se zpracovateli a orgány veřejné správy.

6) Ředitel vede dokumentaci činností a komunikace při reakci na incident tak, aby byla úplná a průkazná.

7) Úkony v reakci na incident se provádějí bez zbytečného odkladu a pokud je to možné, ihned.

8) Hlavními cíli řízení reakce na incident jsou:

a. Ověřit, zda skutečně došlo k porušení zabezpečení osobních údajů.

b. Zjistit, zda došlo k neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů, případně jinému nežádoucímu stavu nebo dopadu.

c. Zamezit možnosti neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů.

d. Zjistit rozsah incidentu.

e. Zjistit, které osoby se mohly neoprávněně s osobními údaji seznámit.

f. Zjistit, kde se osobní údaje a informační systémy nacházejí v rozporu s předpisy organizace a obecně závaznými právními normami.

g. Opatřit důkazy pro řízení, vyšetřování nebo dokazování. Pokud je to třeba, použijí se forenzní metody a standardy.

h. Zjistit, zda je potřebné oznamovat incident třetím stranám.

i. Navrhnout a přijmout taková opatření, aby incident pominul.

j. Navrhnout a přijmout taková opatření, aby se incident neopakoval.

k. Sdílet nebo předat varování třetím osobám, zejména dozorovému úřadu tak, aby se předešlo incidentům u dalších správců.

9) Činnost podle tohoto článku se ukončí, jestliže o tom rozhodne Ředitel na základě předložené zprávy a zabezpečených podkladů a informací, nebo pokud se prokáže, že k incidentu nedošlo. Pokud se prokáže, že k incidentu nedošlo, vypracuje Pověřenec pro ochranu osobních údajů zprávu v obdobném rozsahu.

Článek 22

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

10) Jakékoli porušení zabezpečení osobních údajů organizace jako správce osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděla, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

11) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu organizaci jako správci osobních údajů.

12) Ohlášení případů porušení zabezpečení osobních údajů musí přinejmenším obsahovat:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) jméno a kontaktní údaje Pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

d) popis opatření, která organizace jako správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

13) Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Pověřenec pro ochranu osobních údajů dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Článek 23

Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

1) Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí organizace jako správce osobních údajů toto porušení bez zbytečného odkladu subjektu údajů.

2) V oznámení určeném subjektu údajů se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v čl. 22 této Směrnice.

3) Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) Organizace jako správce osobních údajů 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;

b) Organizace jako správce osobních údajů přijala následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;

c) oznámení by vyžadovalo nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

4) Jestliže organizace jako správce osobních údajů dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámila, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil.

Článek 24

Zpracovatel

1) Pokud má být zpracování provedeno pro organizaci jako správce osobních údajů, využije organizace pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení GDPR a této směrnice a aby byla zajištěna ochrana práv subjektu údajů.

2) Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení organizace jako správce osobních údajů. V případě obecného písemného povolení zpracovatel informuje organizaci jako správce osobních údajů o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak organizaci jako správci osobních údajů příležitost vyslovit vůči těmto změnám námitky.

3) Zpracování zpracovatelem se řídí smlouvou. Zodpovědná osoba je povinna zajistit, aby s každým zpracovatelem byla před zahájením zpracování uzavřena Smlouva o zpracování osobních údajů, která zavazuje zpracovatele vůči organizaci jako správci osobních údajů a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Vzor Smlouvy o zpracování osobních údajů je umístěn na síťovém disku Pythia /ucitele (v digitální podobě) a v kanceláři ředitele školy (v tištěné podobě) .

Článek 25

Kontrola dodržování ustanovení směrnice

1) Vedoucí pracovníci zajistí kontrolu plnění povinností vyplývajících z ustanovení této Směrnice pro nakládání s osobními údaji v mezích své působnosti.

2) Vedoucí pracovníci zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všichni zaměstnanci.

3) Pověřenec je zodpovědný za pravidelné testování, posuzování a hodnocení účinnosti zavedených organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji. Při provádění kontrolních činností jsou všichni zaměstnanci povinni poskytovat Pověřenci součinnost. O provedených zjištěních vede Pověřenec pro ochranu osobních údajů prokazatelnou dokumentaci, kterou předkládá na vědomí řediteli.

4) V případě doporučení ke změnám organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování osobních údajů předkládá Pověřenec tato doporučení řediteli ke schválení.

Článek 26

Revize směrnice

1) Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.

2) Za zpracování, prosazení, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá Pověřenec pro ochranu osobních údajů.

Článek 27

Platnost a účinnost směrnice

1) Dokument Směrnice pro nakládání s osobními údaji předkládá Pověřenec pro ochranu osobních údajů ke schválení řediteli.

2) Dokument Směrnice pro nakládání s osobními údaji nabývá účinnosti a platnosti dnem jejího vydání.

Článek 28

Závěrečná ustanovení

1) Tuto směrnici, všechny její následné změny a doplňky schvaluje Mgr. Milan Fus, ředitel školy. Za její aktualizaci odpovídá Pověřenec pro ochranu osobních údajů.

2) Tato směrnice byla schválena Mgr. Milanem Fusem, ředitelem školy dne 24. 04. 2018.

V Orlové dne 24. 04. 2018

……..

Mgr. Milan Fus
ředitel Základní školy Orlová – Lutyně Ke Studánce 1050 okres Karviná

Příloha - Pravidla pro plnění povinností vůči subjektům údajů

Příjem žádostí

1) Příjem žádostí je prováděn výhradně proti jednoznačné identifikaci subjektu údajů (ztotožnění), tedy podáním žádosti Datovou schránkou nebo ověřením totožnosti předložením občanského průkazu.

2) Je vedena evidence žádostí a poskytnutých odpovědí Subjektu údajů.

Zpracování žádostí

1) Organizace poskytne subjektu údajů na žádost informace, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. Organizace informuje subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

2) Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.

3) Pokud organizace nepřijme opatření, o něž subjekt údajů požádal, organizace informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt údajů o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

4) Informace podle článků a veškerá sdělení a veškeré úkony se poskytují a činí bezplatně. Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může organizace buď:

a) uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů; nebo
b) odmítnout žádosti vyhovět.

Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá organizace.

5) 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.

6) Právem subjektu údajů získat požadované informace nesmějí být nepříznivě dotčena práva a svobody jiných osob (pokud dokument obsahující osobní údaje subjektu údajů obsahuje osobní údaje také jiných subjektů údajů, musí být tyto osobní údaje třetích osob před poskytnutím kopie anonymizovány).

7) Organizace nebo Zpracovatel (po výzvě organizace) provede vyhledání konkrétní osoby v rámci dostupných informačních systémů na základě předaných informací od Subjektu údajů (jméno, příjmení, mobilní telefon, email, rodné číslo, datum narození, místo narození) v rámci

a) Strukturovaných dat – ve vybraných systémech je realizováno speciální funkcionalitou pro práva Subjektu údajů. V ostatních informačních systémech je realizováno nativními funkcemi informačního systému nebo přímým přístupem do databáze.

b) Nestrukturovaných dat – v rámci emailových serverů, sdílených disků je provedeno vyhledání v rámci nativních funkcí jednotlivých informačních systémů.

8) Volba informačních systémů, ve kterých bude vyhledávání realizováno, bude volena s ohledem na skutečnost, zda žadatel je/byl žákem, dodavatelem nebo zaměstnancem.

9) V případě strukturovaných dat je Subjekt nalezen nebo nenalezen. Následně mohou být uplatněna práva ze strany organizace. O výsledku provedení práv, případně nenalezení Subjektu údajů je informován Pověřenec pro ochranu osobních údajů.

10) V případě nestrukturovaných dat je Subjekt nalezen nebo nenalezen. Organizace ve spolupráci s příslušným uživatelem osobních údajů prověří, zda jsou vyhledaná data ztotožnitelná se Subjektem údajů nebo ne. V případech vedení např. IP adres nebude ztotožnění nikdy realizováno s ohledem na nemožnost prověření vazby IP adresy na Subjekt údajů.

11) Výsledek uplatnění práv Subjektu údajů je doplněn o účely zpracování a o seznam Zpracovatelů. Seznam Zpracovatelů je pouze jeden a to pro všechny vedené osobní údaje centrální.

12) Organizace předá konsolidovanou odpověď Subjektu údajů a zavede ji do evidence.

Zpracování žádostí – právo na přístup

1) Právo na přístup je poskytnuto vždy, pokud dojde k nalezení Subjektu údajů v rámci informačních systémů organizace.

2) Součástí odpovědi na právo o přístup jsou vždy exporty ze všech informačních systémů, kde je Subjekt údajů nalezen, účely zpracování jeho osobních údajů a dále seznam Zpracovatelů.

Zpracování žádostí – právo na přenositelnost

1) Právo na přenositelnost je poskytnuto v případě zpracování na základě souhlasu či smlouvy a pouze pro data předaná Subjektem údajů.

2) Součástí odpovědi na právo o přenositelnost jsou exporty v CSV souboru.

Zpracování žádostí – právo na výmaz

1) Právo na výmaz je prováděno automaticky po skončení lhůty pro uchování osobních údajů stanovené v jednotlivých Záznamech o zpracování osobních údajů.

3) Ad-hoc výmaz na základě uplatnění práva na výmaz je realizován pouze v případě zpracování osobních údajů bez právního základu, po uplynutí lhůty pro uchování osobních údajů a v případě neoprávněné evidence a zveřejňování fotografií, pokud je možné provedení ztotožnění Subjektu údajů.

4) Ad-hoc výmaz není prováděn v případě právní povinnosti osobní údaje nadále uchovávat.

5) Ad-hoc výmaz není prováděn v případě vedených cookies, protože zde je identifikátorem Subjektu údajů IP adresa, která není ověřitelná z hlediska ztotožnění Subjektu údajů.

Zpracování žádostí – právo na námitku

1) Právo na námitku je zpracováno vždy podle konkrétní námitky. Realizace tohoto práva není automatizována, jelikož se může jednat o množství různých technicky specifických požadavků vedoucích na data v různých informačních systémech.

2) Námitky, které nemají specifikován dopad na organizaci, organizace konzultuje s Pověřencem pro ochranu osobních údajů.

Zpracování žádostí – právo na aktualizaci vedených osobních údajů

1) Právo na aktualizaci je prováděno selektivně. Na základě požadované aktualizace je provedena skrze přístup běžného pracovníka (aktualizace je vedena shodně jako změna zadávaná přes zaměstnance se zajištěním logování a provedena zaměstnancem s příslušnými právy).

Expedice žádostí

1) Expedice výstupů z provedených práv Subjektu údajů je prováděna

   a) Elektronicky emailovou zprávou na kontaktní email zadaný Subjektem údajů v rámci žádosti.
   b) Doporučeným dopisem, v případě, že Subjekt údajů nezadal kontaktní emailovou adresu.

2) V případě, kdy jsou předmětem odpovědi předávané osobní údaje (Přístup, Přenositelnost), jsou jmenované osobní údaje předávány jako příloha emailu ve formě ZIP. Příloha je zašifrována a heslo k souboru je zasláno Subjektu údajů na jeho mobilní telefon uvedený v žádosti o uvedená práva Subjektu údajů. Heslo musí mít nejméně 10 znaků, nejméně 1 číslici, 1 velké písmeno a 1 speciální znak.

3) O doručení emailu Subjektu údajů s odpovědí na žádost o práva Subjektu údajů musí být uchováno potvrzení o doručení emailové zprávy příjemci (není vyžadována notifikace o přečtení emailové zprávy).

4) Informace o poskytnutí informace o osobních údajích subjektu údajů se zaznamená u dokumentu nebo ve spisu, ve kterém je dokument založen.

5) Pokud nedojde k doručení potvrzení o doručení emailové zprávy, organizace se spojí se Subjektem údajů a potvrdí postup doručení včetně správnosti zadané emailové adresy v rámci žádosti o právo Subjektu údajů.

Prodloužení termínu

1) V případě značného rozsahu vedených dat provede na základě vlastního uvážení organizace prodloužení doby na splnění práva Subjektu údajů o další 2 měsíce.

2) O prodloužení doby na poskytnutí práva Subjektu údajů organizace vždy informuje Pověřence pro ochranu osobních údajů.

3) O prodloužení doby na poskytnutí práva Subjektu údajů organizace vždy informuje Subjekt údajů elektronicky podepsanou emailovou zprávou na kontaktní email zadaný Subjektem údajů v rámci žádosti. O doručení emailu organizace vede potvrzení o doručení emailu.

Záznamy o provedených právech

1) O provedených právech se jsou vedeny auditní stopy decentralizovaně a to

    a) V jednotlivých informačních systémech na úrovni logu (provedení vyhledání subjektu, uplatnění práva).

    b) V elektronické podobě XLS tabulky v rámci vedení statistického přehledu o uplatněných právech a pro potřebu kontroly činnosti ze strany Pověřence.

2) Archivní doba logů v informačních systémech je stanovena na 5 let.