Směrnice „Metodika ochrany osobních údajů“

O B S A H :

1. Úvodní ustanovení

1.1 Předmět

Směrnice stanovuje zásady ochrany osobních údajů fyzických osob podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) - (dále také jen „**GDPR**") a podmínky, za kterých se osobní údaje zpracovávají v organizaci Mateřská škola, Praha 8, Na Korábě 2 (dále také jen „**Škola**" nebo „**Organizace**").

1.2 Cíl

Touto směrnicí se stanovují takové postupy, které mají zajistit, aby v Organizaci a u jejích Zpracovatelů byly zpracovávány osobní údaje v souladu s GDPR a aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změnám, zničení, ztrátám, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, nebo i k jinému zneužití.

1.3 Rozsah platnosti

Tato směrnice je závazná pro všechny zaměstnance Organizace a osoby v obdobném vztahu k Organizaci, které se podílejí na zpracování osobních údajů v Organizaci. Směrnice je rovněž závazná pro subjekty, které byly Organizací pověřeny ke zpracování osobních údajů.

1.4 Pojmy a definice

Pro účely této směrnice platí následující definice a zkratky, a to bez ohledu na to, zda jsou psány s malým či velkým počátečním písmenem:

Bezpečnostní incident – porušení zabezpečení, které může vést k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Blokování osobních údajů – je vytvoření takového stavu, při kterém je osobní údaj po určitou dobu nepřístupný a nelze jej jinak zpracovávat.

Citlivý údaj – osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

DPO – pověřenec pro ochranu osobních údajů (Data Protection Officer) je osoba, která u Organizace zajišťuje a kontroluje soulad činnosti Organizace s GDPR a touto Směrnicí.

Evidence osobních údajů – jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

Fyzická ochrana – je komplex technických, režimových a organizačních opatření a ostrahy, jejichž cílem je minimalizace rizik vyplývajících z neoprávněných činností s majetkem, nebo které mají za cíl zajistit bezpečnost osob.

Garant zpracování OÚ – pověřený zaměstnanec Organizace, který zaručuje správnost evidence oblastí zpracování OÚ v Organizaci.

Identifikovatelná osoba – 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.

Informační povinnost – naplnění povinnosti správce vůči subjektu údajů spočívající v poskytnutí informací nezbytných pro subjekty údajů.

Likvidace osobních údajů – se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.

Neoprávněné nakládání s osobními údaji – je zejména jejich vyzrazení, zneužití, poškození, znehodnocení, neoprávněná likvidace, porušení jejich ochrany nebo ztráta.

Nosné médium osobního údaje – prostředek, který umožňuje udržování osobního údaje v podobě, která umožňuje jej dále zpracovávat. Může mít listinnou podobu nebo jinou hmotnou podobu nebo to může být elektronické médium, které je pevnou nebo oddělitelnou, přenosnou nebo nepřenosnou součástí počítačového systému.

Oprávněná osoba – zaměstnanec (nebo fyzická osoba v jiném než pracovním poměru k Organizaci), který při plnění pracovních úkolů zpracovává osobní údaje.

Osobní údaj – veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

Písemnost – listina, nosné médium a jiný materiál, obsahující osobní údaje vyjádřené v jakékoli podobě.

Příjemce OÚ – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu nebo nikoliv.

Rodné číslo – identifikátor fyzické osoby, přidělovaný v souladu se zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů, případně obecně závazný právní přepis tento zákon nahrazující.

Shromažďování osobních údajů – je systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosné médium osobního údaje pro jejich okamžité nebo pozdější zpracování.

Směrnice – tato směrnice „Metodika ochrany osobních údajů“.

Souhlas subjektu údajů – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či zjevným potvrzením své povolení ke zpracování svých osobních údajů.

Správce – subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Správce může zmocnit nebo pověřit zpracováním osobních údajů Zpracovatele.

Subjekt údajů – je fyzická osoba, k níž se osobní údaje vztahují. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu.

Uchovávání osobních údajů – je udržování údajů v takové podobě, která je umožňuje dále zpracovávat.

Úřad – Úřad pro ochranu osobních údajů, kterému jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů.

Zachování mlčenlivosti – povinnost nezpřístupňovat osobní údaje a informace o opatřeních k jejich zabezpečení osobě, která není oprávněna se s osobními údaji seznamovat.

Zaměstnanec – fyzická osoba, která na základě uzavřené pracovní smlouvy pracuje u Správce v pracovním poměru nebo je ke Správci v jiném pracovněprávním vztahu.

Zpracování osobních údajů – 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, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zpracovatel – je fyzická nebo právnická osoba, orgán veřejné moci, agentura či jiný subjekt, která zpracovává osobní údaje pro správce na základě písemné smlouvy o zpracování osobních údajů.

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

1.5 Zkratky

DPO	Pověřenec pro ochranu osobních údajů **(**Data Protection Officer**)**
GZOÚ	Garant zpracování osobních údajů
OO	Oprávněná osoba
OÚ	Osobní údaj
SÚ	Subjekt údajů
ÚOOÚ	Úřad pro ochranu osobních údajů

2. Způsoby zajištění ochrany osobních údajů

Pro ochranu osobních údajů má Organizace přijata taková bezpečnostní opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Těmito bezpečnostními opatřeními jsou opatření v oblasti:

- personální bezpečnosti;
- fyzické ochrany;
- informační a komunikační bezpečnosti;
- administrativní bezpečnosti.

3. MATICE ODPOVĚDNOSTI

3.1 Matice odpovědnosti procesu

S spolupracuje se zodpovídajícím
Z zodpovídá

Činnost	Odpovědnost		
	DPO	**ředitel**	**OO**
Zajištění kontroly a souladu činností organizace s GDPR a touto Směrnicí, posouzení rizik.	S	Z	S
Vedení celkového přehledu o oblastech zpracování OÚ (vč. návrhu „stanovení“ oblastí zpracování OÚ a odpovědného garanta zpracování OÚ.)	Z		
Odpovídá za způsob dokumentování a udržování „systému“ dokumentace zpracování OÚ v Organizaci.	S	Z	
Zajištění školení o postupech ochrany osobních údajů v rozsahu potřebném k výkonu činností jednotlivých zaměstnanců.	Z	S	S
Nastavení pravidel a realizace Informační povinnosti transparentním, srozumitelným a dostupným způsobem.	S	Z	
Uzavření smlouvy o zpracování OÚ.		Z	S
Vytvoření a udržování systému ochrany osobních údajů v Organizaci.	S	Z	
Řízení procesu ochrany osobních údajů v Organizaci.	Z	Z	S
Řešení bezpečnostních incidentů vzniklých v souvislosti s ochranou osobních údajů, analýza jejich příčin a navrhování nápravných opatření.	S	S	Z
Stanovení účelu zpracovávání osobních údajů, rozsahu zpracovávaných osobních údajů, určení zdroje osobních údajů (způsob získávání), místa, způsobu a dalších okolností zpracovávání osobních údajů.	S	Z	S
Seznámení všech zaměstnanců s touto směrnicí a stanovení úkolů k naplnění této směrnice.	S	Z	
Stanovení způsobu, prostředků a místa zpracování osobních údajů, včetně povinností a odpovědnosti jednotlivých Oprávněných osob.	S	Z	

Činnost	Odpovědnost		
	DPO	ředitel	OO
Zajištění ochrany a bezpečnosti osobních údajů v souladu s GDPR a touto směrnicí, a to od zahájení jejich zpracovávání až do chvíle, kdy jsou likvidovány.	S	Z	S
Zajištění skutečnosti, že osobní údaje budou shromažďovány v Organizaci pouze pro stanovený účel a právní titul.	S	Z	Z
Zajištění toho, že v Organizaci budou osobní údaje uchovávány pouze po stanovenou dobu.	S	Z	S
Zabezpečení zpracovávání osobních údajů v Organizaci v souladu s účelem, k němuž byly shromážděny, a pokud by měly být osobní údaje použity k jinému účelu, zabezpečit získání souhlasu Subjektu údajů.	S	Z	Z
Zajištění shromažďování osobních údajů v Organizaci pouze otevřeně, nikoliv pod záminkou jiného účelu nebo jiné činnosti.	S	Z	S
Zabezpečit, aby nebyly v organizaci sdružovány osobní údaje, které byly získány s rozdílným účelem.	S	Z	Z
Dodržování pravidel stanovených touto směrnicí, plnění úkolů a pokynů.	Z	Z	Z
Zpracování osobních údajů v souladu s účelem, ke kterému byly shromážděny a v rozsahu nezbytném pro naplnění stanoveného účelu.	S	Z	S

4. Ochrana osobních údajů v Organizaci

4.1 Subjekty údajů

1. Typickými Subjekty údajů v podmínkách Školy jsou:
   - fyzické osoby v zaměstnaneckém nebo obdobném vztahu,
   - třetí osoby, které nemusí být ve vztahu s Organizací (např. návštěvy, exkurze, rodinní příslušníci zaměstnanců, účastníci pojistných událostí bez vztahu k Organizaci),
   - dodavatelé Organizace, tj. (fyzické osoby) nebo zástupci dodavatelů (u právnických osob) (např. správci informačních technologií apod.),
   - uchazeči o zaměstnání v Organizaci,
   - děti, zákonní zástupci.
2. V souvislosti s identifikací Subjektu údajů je třeba posoudit, jaký je účel zpracovávání (z jakého důvodu je prováděno) a zda je ke zpracovávání nutný souhlas Subjektu údajů.
3. Dále je nutné stanovit způsob získávání osobních údajů od fyzických osob, zejména s ohledem na to, aby nedocházelo k využívání údajů získaných k jinému účelu, případně ke slučování údajů získaných k jiným účelům, a způsob plnění informační povinnosti správce vůči subjektu údajů.

4.2 Zpracování osobních údajů

4.2.1. Účel zpracovávání

Ředitel školy stanoví účel zpracování osobních údajů a rozsah využívaných údajů. Stanovený účel zpracovávání musí být pravdivý a jednoznačný.

Osobní údaje lze zpracovávat pouze v souladu s účelem, k němuž byl shromážděn.

4.2.2. Rozsah zpracovávaných údajů

Rozsah zpracovávaných osobních údajů musí být stanoven tak, aby splnil svůj účel, a přitom nebyly shromažďovány a zpracovávány nadbytečné osobní údaje.

4.2.3. Zdroje osobních údajů

Zdrojem pro zpracování osobních údajů jsou primárně údaje poskytnuté SÚ (a ověřené OO).

4.2.4. Místo a způsob zpracovávání, opatření k ochraně osobních údajů

Ředitel školy stanoví místa, na kterých jsou OÚ zpracovávány, prostředky a způsob (technologie), které jsou ke zpracovávání využívány.

Ředitel školy stanoví personální, administrativní a režimová opatření sloužící k zajištění ochrany OÚ, které zpracovává.

OO může zahájit zpracování OÚ jen za předpokladu, že jsou splněny veškeré podmínky stanovené GDPR, tj. je zejména splněna informační povinnost vůči SÚ, existuje právní titul ke zpracování.

4.2.5. Posouzení vlivu na ochranu osobních údajů

DPO je povinen při jakékoliv změně procesu zpracování OÚ nebo novém zpracování provést posouzení možných dopadů na práva a svobody SÚ vyplývajících z prováděného zpracování (PI – dopad na subjekty údajů). V případě, že toto posouzení indikuje vysokou míru rizika pro SÚ anebo GDPR vyžaduje detailní analýzu, DPO zpracuje celkové posouzení dopadu na ochranu OÚ (DPIA dle GDPR). DPIA obsahuje celkové posouzení hrozeb/rizik zpracování a úrovně opatření směřujících proti hrozbám.

Posouzení vlivu na ochranu OÚ musí provést DPO zejména když se jedná o:

a) systematické a rozsáhlé vyhodnocování OÚ fyzických osob, které je založeno na automatizovaném zpracování, profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k SÚ právní účinky nebo mají na SÚ závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů nebo OÚ týkajících se rozsudků v trestních věcech a trestných činů;

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

4.2.6. Podmínky pro Konzultace s dozorovým orgánem

DPO musí konzultovat zpracování s dozorovým orgánem v případě, že z posouzení vlivu na ochranu OÚ (DPIA) vyplývá, že by dané zpracování mělo za následek vysoké riziko pro SÚ i přes přijetí opatření ke zmírnění rizika nebo v případě, kdy není možné přijmout žádné opatření ke zmírnění rizika.

Při konzultaci s dozorovým orgánem musí DPO poskytnout přinejmenším následující informace:

- rozdělení odpovědnosti mezi Organizací, společnými správci a zpracovateli zapojenými do zpracování;
- účely a způsoby zamýšleného zpracování;
- zamýšlená opatření za účelem ochrany práv a svobod SÚ;
- kontaktní údaje.

4.2.7. Posuzování změn v Organizaci

Veškeré změny v procesech Organizace s vlivem na ochranu OÚ musí být řízené. Musí být popsány a musí být posouzeny DPO z pohledu dopadu změny do procesu ochrany OÚ. Bez schválení změny DPO nesmí být provedena žádná změna procesů zpracování OÚ.

4.2.8. Vedení Záznamů zpracování

Odpovědností DPO je vést „Záznamy zpracování“. Odpovědností GZOÚ je spolupracovat a dodat DPO podklady ke zpracování „Záznamu zpracování“. Tento záznam musí přinejmenším obsahovat:

a) jméno a kontaktní údaje Organizace a DPO;

b) účely zpracování;

c) popis kategorií SÚ a kategorií OÚ;

d) kategorie příjemců, kterým byly nebo budou OÚ zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;

e) informace o případném předání OÚ do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání doložení vhodných záruk;

f) plánované lhůty pro výmaz jednotlivých kategorií osobních údajů v případě, že je možné je stanovit;

g) obecný popis technických a organizačních bezpečnostních opatření uvedených pro ochranu OÚ.

DPO je odpovědný za komunikaci s dozorovým úřadem a je povinen poskytnout záznamy na požádání dozorovému úřadu.

4.2.9. Kategorie osobních údajů

Všechny kategorie OÚ zpracovávané v Organizaci jsou součástí „Záznamů zpracování“.

4.3 Právní tituly ke zpracování

Všechny právní tituly zpracování v Organizaci v návaznosti na jednotlivé oblasti zpracování jsou zpracovány v „Záznamech zpracování“.

I. Subjekt údajů udělil souhlas se zpracováním osobních údajů

V případě, že zpracování OÚ je založeno na souhlasu subjektu údajů, Garant zpracování OÚ odpovídá za nastavení pravidel, která zajistí:

a) získání souhlasu SÚ se zpracováním OÚ, a to v okamžiku shromáždění údajů,

b) udělení souhlasu SÚ bude doložitelné po celou dobu zpracování OÚ,

c) před udělením souhlasu bude SÚ informován o způsobech zpracování OÚ,

d) případné odvolání souhlasu bude stejně snadné jako jeho poskytnutí.

Náležitosti uděleného souhlasu jsou uvedeny níže a vzor souhlasu je obsažený v dokumentu souhlas se zpracováním OÚ:

a) “souhlasím se zpracování svých osobních údajů";

b) identifikace správce OÚ;

c) identifikace dalších správců (pokud se uplatní);

d) účel zpracování;

e) souhlas/data poskytnuty dobrovolně;

f) doba zpracování, resp. způsob, jak se doba určí;

g) předávání údajů třetím stranám (pokud se uplatní);

h) právo souhlas kdykoliv odvolat;

i) právo na přístup;

j) právo na opravu chyb a nepřesností;

k) právo na výmaz;

l) odkaz na další informace o zpracování (zásady zpracování osobních údajů/ privacy policy).

V podmínkách Organizace je za souhlas se zpracováním OÚ považováno:

a) v listinné podobě – uvedením vlastnoručního podpisu subjektu údajů, včetně data podpisu,

b) v elektronické formě - např. připojením el. podpisu, dále též zaškrtnutím příslušného pole v elektronickém formuláři, příp. další způsoby dle dokumentace zpracování OÚ.

Souhlas musí být prokazatelný po celou dobu zpracování OÚ. Pokud subjekt údajů souhlas neposkytne ani k tomu není jiný právní titul, nelze OÚ zpracovávat.

Všechny právní tituly zpracování v Organizaci v návaznosti na jednotlivé oblasti zpracování jsou zpracovány v Záznamech zpracování.

II. Zpracování je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů

Jedná se např. o shromažďování osobních údajů SÚ v systému pro stravování.

III. Zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje

Jedná se o sběr všech osobních údajů v souvislosti s poskytováním předškolního vzdělávání dětí, docházky do zaměstnání apod.

IV. Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby

V Organizaci se tento právní titul nevyužívá.

V. Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen Správce

V Organizaci se tento právní titul nevyužívá.

VI. Zpracování je nezbytné pro účely oprávněných zájmů Organizace

4.4 Informační povinnost dle č. 13 a 14 GDPR

V případě, kdy Organizace shromažďuje OÚ přímo od subjektu údajů, musí být subjektu údajů poskytnuty přinejmenším následující informace o zpracování OÚ v okamžiku získání:

Totožnost a kontaktní údaje správce,

a) Kontaktní údaje na DPO.
b) Účel, pro který jsou OÚ zpracovávány, a právní titul tohoto zpracování.
c) Oprávněné zájmy správce nebo třetí strany – v případě, že je zpracování založeno na tomto právním titulu.
d) Případné příjemce nebo kategorie příjemců (pokud jim budou OÚ předávány).
e) Případný úmysl předat OÚ do třetí země.

Dále subjektu údajů musí být poskytnuty následující informace:

a) Doba, po kterou budou OÚ uloženy, příp. kritéria pro stanovení této doby.
b) Existence práva požadovat od správce přístup k OÚ týkající se subjektu údajů.
c) Existence práva kdykoliv odvolat souhlas se zpracováním, pokud je souhlas právním základem pro zpracování.
d) Existence práva podat stížnost u dozorového úřadu.

e) Skutečnost, zda poskytování OÚ je zákonným nebo 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 (rozhodování, které provádí stroj na základě stanovených kritérií bez vlivu člověka), včetně profilování, přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

V případě, že OÚ nebyly získány od subjektu údajů, musí správce subjektu údajů poskytnout tyto informace:

a) Totožnost a kontaktní údaje správce a případně jeho zástupce.

b) Kontaktní údaje pověřence pro ochranu osobních údajů.

c) Účely zpracování, pro které jsou osobní údaje určeny, a právní titul pro zpracování.

d) Kategorie dotčených osobních údajů.

e) Případné příjemce nebo kategorie příjemců osobních údajů.

f) Případný záměr správce předat osobní údaje příjemci ve třetí zemi.

Dále subjektu údajů musí být poskytnuty následující informace:

a) Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na tomto právním titulu.

b) Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů.

c) Pokud je zpracování založeno na subjektem údajů uděleném souhlasu, existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním.

d) Zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů.

Za nastavení pravidel a realizaci Informační povinnosti transparentním, srozumitelným a dostupným způsobem odpovídá Garant zpracování OÚ. V této oblasti poskytuje součinnost DPO.

4.5 Seznamy zpracovávaných osobních údajů

4.5.1. Seznam osobních údajů zpracovávaných v Organizaci

Jednotlivé kategorie osobních údajů jsou využívány různě v jednotlivých oblastech zpracování. Přesný rozpis použitých kategorií osobních údajů je uveden v „Záznamech zpracování“.

Garant zpracování OÚ je odpovědný za průběžnou aktualizaci seznamu kategorií osobních údajů zpracovávaných v dané oblasti. Aktualizovaný seznam předává DPO, který zodpovídá za celkovou aktualizaci „Záznamů zpracování“.

4.5.2. Záznamy zpracování

OÚ jsou zpracovávány jako součást činnosti (resp. agendy) Organizace. Oprávněná osoba Organizace určuje účel, způsob a další parametry zpracování OÚ.

Z pohledu hlavních „agend“ Organizace, z hlediska kategorie dotčených subjektů OÚ a dále pro potřeby řízení, je zpracování OÚ v Organizaci členěno na oblasti zpracování OÚ.

Celkový přehled o oblastech zpracování OÚ v Organizaci vede DPO, který navrhuje vedení Organizace „stanovení“ oblastí zpracování OÚ a odpovědného Garanta za zpracování. Oblasti zpracování OÚ jsou stanovovány dle potřeb Organizace s cílem co nejefektivněji řídit zpracování OÚ a zajišťovat soulad s platnou legislativou.

Způsoby a parametry zpracování OÚ v dané oblasti musí být vždy popsáno v řídící dokumentaci. Za vedení a udržování dokumentace zpracování OÚ v aktuálním stavu odpovídá Garant zpracování OÚ.

Za způsob dokumentování a udržování systému dokumentace zpracování OÚ v Organizaci odpovídá DPO.

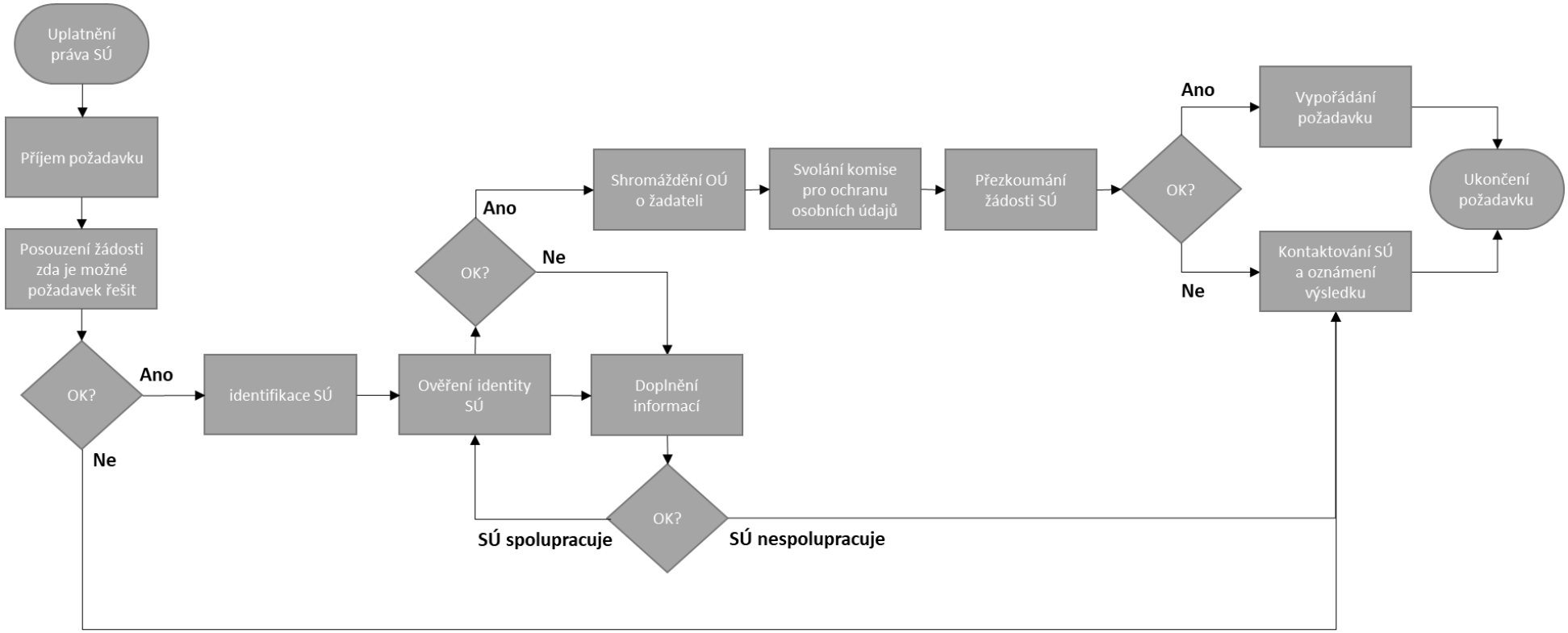
4.6 Uplatnění práv ze strany subjektů údajů

4.6.1. Práva subjektů údajů

Práva subjektů údajů jsou stanovena GDPR. Zejména se jedná o následující práva:

- právo na přístup (čl. 15 GDPR),
- právo na opravu (čl. 16 GDPR),
- právo na výmaz / být zapomenut (čl. 17 GDPR),
- právo na omezení zpracování (čl. 18 GDPR),
- právo na přenositelnost (čl. 20 GDPR),
- právo vznést námitku (čl. 21 GDPR).

4.6.2. Proces uplatňování práv subjektů údajů


Uplatnění práva SÚ
Příjem požadavku
Posouzení žádosti zda je možné požadavek řešit
OK?
Ano
Ne
identifikace SÚ
Ověření identity SÚ
OK?
Ano
Ne
Shromáždění OÚ o žadateli
Svolání komise pro ochranu osobních údajů
Přezkoumání žádosti SÚ
OK?
Ano
Ne
Vypořádání požadavku
Kontaktování SÚ a oznámení výsledku
Ukončení požadavku
Doplnění informací
OK?
SÚ spolupracuje
SÚ nespolupracuje

Všeobecné činnosti související s uplatněním níže uvedených práv subjektu údajů jsou:

#	Činnost	Popis činnosti	Odpovědná osoba
0	*<všeobecné činnosti týkající se práv subjektů údajů>*		
1	Přijetí žádosti	• Informace o přijaté žádosti jsou shromážděny a zpracovávány u GZOÚ. Pokud se žádost dostane jinam, je okamžitě předána GZOÚ.	
2	Identifikace subjektu údajů	• Organizace vhodným způsobem prověřuje a jasně určuje totožnost subjektu údajů.	
3	Přezkoumání žádosti a povinnosti spolupráce subjektu údajů	• Organizace kontroluje, zda není žádost zjevně neopodstatněná nebo přehnaná. • Organizace rovněž přezkoumává, zda byla žádost subjektu údajů jasně a prokazatelně oznámena a zda subjekt údajů splnil svou povinnosti spolupráce. • Lhůta pro přezkoumání žádosti je 30 dní.	
4	Kontrola zákonnosti požadavku	• Organizace prověřuje, zda existují oprávněné důvody pro odmítnutí námitek	
5	Identifikace osobních údajů	• Organizace identifikuje osobní údaje subjektu údajů, které zpracovávají.	

6	Kontrola, zda existuje potřeba osobní údaje i nadále zpracovávat	• Organizace kontroluje, zda je zpracování osobních údajů subjektu údajů vyžadováno GDPR. To může být případ, pokud jsou osobní údaje požadovány pro následující případy:
		  • povinnost vzhledem k občanskému právu;
		  • daňové povinnosti;
		  • příkazy státního zastupitelství pro předávání údajů v rámci trestního řízení;
		  • předpisy dozorového úřadu.	

7	Kontrola, zda existují oprávněné důvody pro zpracování osobních údajů	• V případě legitimní námitky Organizace prověřuje, zda je třeba nadále zpracovávat osobní údaje subjektu údajů. To může nastat pokud:
		  • existují oprávněné důvody pro zpracování, které převažují nad zájmy, právy a svobodami subjektu údajů nebo
		  • zpracování slouží k výkonu nebo obhajobě právních nároků.	

8	Vlastní vyřízení konkrétního práva SÚ	• Není-li potřeba nebo neexistuje-li oprávněný zájem, Organizace zajišťuje, aby dalšímu přístupu a zpracování osobních údajů subjektu bylo zabráněno vymazáním nebo jejich omezením. To zahrnuje také zálohovací nebo testovací systémy nebo osobní údaje pro zpracovatele.	
9	Dokumentace a zajištění zpětné sledovatelnosti požadavku	• Organizace jasně dokumentuje jakoukoli komunikaci se subjektem údajů, jakož i související interní činnosti a přijatá opatření. To zahrnuje důkaz technických a organizačních opatření přijatých s cílem zabránit dalšímu zpracování zrušených osobních údajů.	
10	Komunikace vůči subjektům údajů	• Organizace sděluje přijatá opatření subjektům údajů.	

Lhůta od identifikace subjektu údajů do přijetí opatření (vypořádání) musí být kratší než 30 dní. V případě, že Organizace není schopna v této lhůtě uplatnění práva SÚ vypořádat, musí SÚ informovat o prodloužení termínu na maximálně 60 dní.

4.6.3. Právo na přístup k informacím a poskytnutí kopie osobních údajů

Subjekt údajů má právo získat od správce 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:

- účely zpracování OÚ,
- kategorie dotčených osobních údajů (např. jméno, příjmení, datum narození, adresa apod.),
- příjemci, kterým osobní údaje byly, jsou nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy,
- právo podat stížnost u dozorového úřadu,
- právo žádat o soudní ochranu, pokud nebude žádosti o právo na přístup vyhověno,
- veškeré dostupné informace o zdroji OÚ, pokud nejsou získány od subjektu údajů,
- skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

Proces na uplatnění práva subjektu údajů na přístup k informacím zajišťuje, že požadavky na informace jsou strukturované a srozumitelné. Tím je zajištěno, že v případě legitimní žádosti subjekt údajů obdrží včas oznámení, zda Organizace zpracovává osobní údaje, a v případě potřeby obdrží informace o zpracovávaných osobních údajích.

4.6.4. Právo na výmaz („být zapomenut“)

Právo na výmaz ukládá správci OÚ povinnost bez zbytečného odkladu vymazat OÚ, pokud je dán jeden z těchto důvodů:

- OÚ již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány,
- SÚ odvolá souhlas (zpracování založené na souhlasu), a neexistuje žádný další právní důvod pro zpracování,
- SÚ vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích, a neexistují žádné převažující oprávněné důvody pro zpracování
- osobní údaje byly zpracovávány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené právem Unie nebo právními předpisy České republiky.

Právo na výmaz se naopak neuplatní, pokud je zpracování osobních údajů nezbytné:

- pro splnění právní povinnosti Organizace, jež vyžaduje zpracování podle práva Unie nebo právních předpisů České republiky,
- pro určení, výkon nebo obhajobu právních nároků Organizace.

Proces na uplatnění práva subjektu údajů na výmaz zajišťuje, že požadavky na výmaz jsou strukturované a srozumitelné. Tím je zajištěno, že v případě legitimní žádosti budou osobní údaje subjektu údajů včas vymazány, nebo v případě zveřejnění osobních údajů budou všichni správci, kteří tyto osobní údaje zpracovávají, informováni o uplatnění práva na výmaz.

Právo na výmaz je uplatnitelné, pokud je dán některý z důvodů dle GDPR, zejména pokud došlo ze strany subjektu údajů k odvolání souhlasu, na jehož základě byly osobní údaje zpracovávány a neexistuje žádný další právní důvod zpracování. Obdobně je tomu v případě, kdy subjekt údajů vznese námitky proti zpracování, a neexistují žádné převažující oprávněné důvody pro zpracování.

Zpracováním žádosti tohoto typu je v Organizaci zodpovědný DPO, který je vyškolen na celý proces, včetně komunikace a spolupráce s dotčenými zaměstnanci, do jejichž kompetence předmětná oblast žádosti spadá.

4.6.5. Právo vznést námitku

SÚ má právo kdykoli vznést námitku proti zpracování osobních údajů. Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů.

SÚ musí být na právo vznést námitku upozorněn a toto právo musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se SÚ.

Proces na uplatnění práva subjektu údajů vznést námitky zajišťuje, že námitky (zejména ve vztahu k profilování nebo automatizovanému rozhodování) v Organizaci jsou strukturované a srozumitelné. Tím je zajištěno, že zpracování osobních údajů bude zastaveno v případě legitimní žádosti v závislosti na nutnosti dalšího zpracování a v případě potřeby budou údaje vymazány nebo zablokovány.

Zpracováním žádosti tohoto typu je v Organizaci zodpovědný DPO, který je vyškolen na celý proces, včetně komunikace a spolupráce s dotčenými zaměstnanci, do jejichž kompetence předmětná oblast žádosti spadá.

4.6.6. Právo na omezení zpracování osobních údajů

Právo na omezení umožňuje subjektu údajů žádat omezení zpracování OÚ po určitou dobu (např. dočasný přesun vybraných údajů do jiného systému zpracování (archiv), znepřístupnění konkrétních osobních údajů, stažení zveřejněných údajů z webu apod.). Důvody pro omezení zpracování jsou následující:

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

V informačních systémech, kde se OÚ zpracovávají, by mělo být omezení zpracování zajištěno vhodnými technickými prostředky tak, aby se na OÚ po dobu omezení nevztahovaly žádné další operace zpracování, a tedy aby OU nemohly být změněny. Omezení zpracování OÚ by mělo být v systému jasně vyznačeno.

Proces na omezení zpracování osobních údajů zajišťuje, že se na osobní údaje nebudou do budoucna vztahovat žádné další operace zpracování.

Právo na omezení je uplatnitelné, pokud byl splněn důvod GDPR, zejména pokud a) subjekt údajů popírá přesnost osobních údajů, b) zpracování je protiprávní a subjekt údajů odmítá výmaz, c) správce 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. Ve všech těchto případech má subjekt údajů právo na to, aby správce omezil zpracování.

Zpracováním žádosti tohoto typu je v Organizaci zodpovědný DPO, který je vyškolen na celý proces, včetně komunikace a spolupráce s dotčenými zaměstnanci, do jejichž kompetence předmětná oblast žádosti spadá.

4.6.7. Právo na opravu osobních údajů

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.

Proces na uplatnění práva subjektu údajů na opravu osobních údajů zajišťuje, že v případě žádosti subjektu údajů na opravu nepřesných osobních údajů budou tyto osobní údaje Organizací bez zbytečného odkladu opraveny.

Zpracováním žádosti tohoto typu je v Organizaci zodpovědný DPO, který je vyškolen na celý proces, včetně komunikace a spolupráce s dotčenými zaměstnanci, do jejichž kompetence předmětná oblast žádosti spadá.

4.6.8. Právo na přenositelnost osobních údajů

SÚ má právo získat OÚ, které se ho týkají a jež v minulosti poskytl Organizaci a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. SÚ musí tyto OÚ obdržet ve strukturovaném, běžně používaném a strojově čitelném formátu, a to v případě, že OÚ jsou automatizovaně zpracovávány na základě uděleného souhlasu nebo na základě uzavřené smlouvy.

V rámci práva na přenositelnost má SÚ právo na to, aby osobní údaje byly předány přímo jedním správcem správci jinému, je-li to technicky proveditelné. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

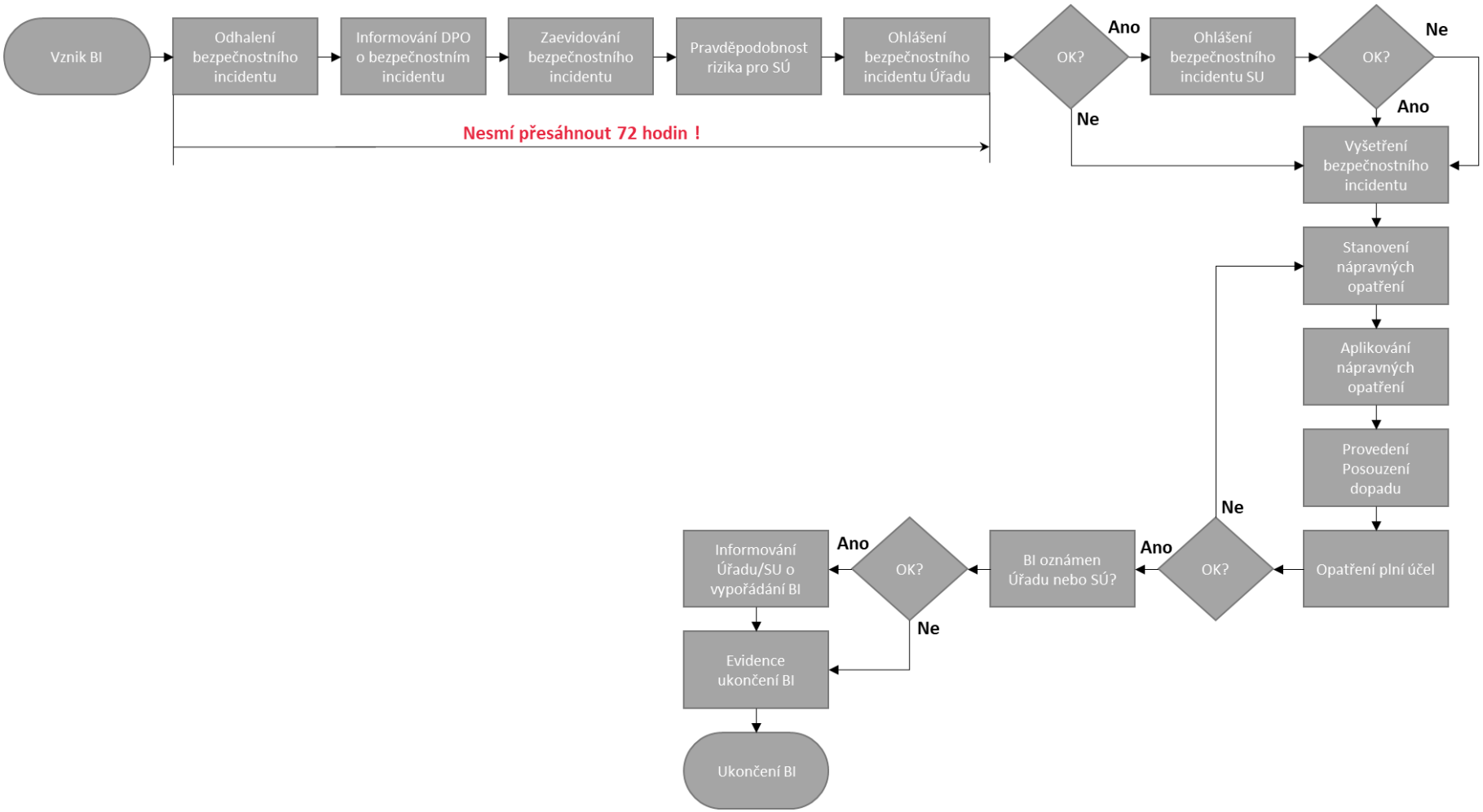
Proces na uplatnění práva subjektu údajů na přenositelnost osobních údajů zajišťuje, že za určitých podmínek má subjekt údajů právo získat osobní údaje, které se ho týkají a jež Organizaci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, včetně práva předat tyto údaje jinému správci. Subjektem údajů může být toto právo uplatněno za splnění dvou podmínek, které musí nastat současně: a) zpracování je založeno na souhlasu subjektu údajů nebo na smlouvě, b) je prováděno automatizovaně.

Zpracováním žádosti tohoto typu je v Organizaci zodpovědný DPO, který je vyškolen na celý proces jejich zpracování, včetně komunikace a spolupráce s dotčenými zaměstnanci, do jejichž kompetence předmětná oblast žádosti spadá.

4.7 Hlášení bezpečnostních incidentů

Hlášení incidentů Úřadu pro ochranu osobních údajů a případně subjektům osobních údajů.

Proces definuje postup ochrany údajů v případě vzniku bezpečnostních incidentů v Organizaci. Zkoumá, zda existuje oznamovací povinnost vůči Úřadu pro ochranu osobních údajů a subjektům údajů a zda jsou dodržovány lhůty.


Vznik BI
Odhalení bezpečnostního incidentu
Informování DPO o bezpečnostním incidentu
Zaevidování bezpečnostního incidentu
Pravděpodobnost rizika pro SÚ
Ohlášení bezpečnostního incidentu Úřadu
OK?
Ano
Ne
Ohlášení bezpečnostního incidentu SU
OK?
Ne
Ano
Nesmí přesáhnout 72 hodin !
Vyšetření bezpečnostního incidentu
Stanovení nápravných opatření
Aplikování nápravných opatření
Provedení Posouzení dopadu
Opatření plní účel
OK?
Ano
Ne
BI oznámen Úřadu nebo SÚ?
OK?
Ano
Ne
Informování Úřadu/SU o vypořádání BI
Evidence ukončení BI
Ukončení BI

#	Činnost	Popis činnosti	Odpovědná osoba
0	*<všeobecné činnosti týkající se práv subjektů údajů>*		
1	Detekce nebo příjem informace o bezpečnostním incidentu	• Bezpečnostní incident je zjištěn interně (zaměstnancem) nebo externě (byla přijata zpráva např. od subjektu údajů/zpracovatele apod.). • Aby byly dodrženy zákonné lhůty, je dokumentován čas, kdy došlo ke zjištění porušení údajů.	
2	Kontrola, zda byl narušením dat ovlivněn zpracovatel	• Organizace kontroluje, zda je narušením dat ovlivněn zpracovatel, a pokud ano, musí být informován.	
3	Aktivace systému hlášení	• Organizace informuje relevantní zaměstnance o potřebě zpracovat bezpečnostní incident a zkontrolovat, zda by měla být svolána specializovaná organizační skupina (např. bezpečnostní výbor).	
4	Vyhodnocení incidentu dle definovaných testovacích metod	• Aby bylo možné posoudit rozsah incidentu a přijmout následná opatření, je únik údajů důkladně prozkoumán na základě definovaného postupu. • Organizace prověřuje technická a organizační opatření účinná v době bezpečnostního incidentu.	
5	Kontrola implementace úvodních opatření	• Organizace prověřuje, zda mohou být provedena opatření přijatá k následnému odstranění rizika práv a svobod subjektů údajů.	
6	Kontrola, zda je třeba zaslat oznámení Úřadu pro ochranu osobních údajů	• Organizace prověřuje, zda je povinna hlásit Úřadu pro ochranu osobních údajů porušení bezpečnosti OÚ.	
7	Kontrola, zda musí být subjektu údajů odesláno oznámení	• Organizace prověřuje, zda je povinna oznámit únik osobních údajů subjektům údajů.	
8	Vyřešení bezpečnostního incidentu	• Organizace zpracovává a řeší incident pomocí vnitřně definovaných postupů – reakce na incidenty. To znamená, že Organizace přijímá nezbytná technická a organizační opatření k obnovení stavu ochrany dotčených osobních údajů.	
9	Implementace opatření pro neustálé zlepšování	• Organizace získává informace o úniku osobních údajů a přijímá následná opatření ke zlepšení ochrany osobních údajů a odhalování dalších incidentů.	
10	Dokumentování a zajištění zpětné sledovatelnosti požadavku	• Organizace srozumitelně dokumentuje jakoukoli komunikaci při zpracování bezpečnostního incidentu, jakož i související interní činnosti a přijatá opatření.	

4.8 Zpracování pomocí zpracovatele

Ke zpracovávání osobních údajů je možno využít externího dodavatele – Zpracovatele. Podmínkou je uzavření písemné smlouvy o zpracovávání osobních údajů mezi Organizací a Zpracovatelem.

Za uzavření smlouvy o zpracování osobních údajů obecně odpovídá ředitel Organizace. V organizaci je možné po souhlasu DPO o požadavky na zpracování osobních údajů rozšířit existující smlouvy uzavírané se Zpracovatelem (např. smlouva o poskytování služeb - účetnictví, IT apod.) či dodatkovat stávající smlouvy.

Zpracováním osobních údajů prostřednictvím Zpracovatele není dotčeno právo Organizace stanovit oprávnění přístupu k osobním údajům jak pro své zaměstnance, tak pro třetí osoby.

Zpracovatel není oprávněn zpracovávat osobní údaje k jinému účelu a jiným způsobem než smluvně dohodnutým. Stejně tak není oprávněn předávat nebo zpřístupňovat zpracovávané osobní údaje jiným osobám než určenými Organizací.

4.9 Doba uchovávání osobních údajů

Doba uchování/zpracování osobních údajů je pro každou oblast zpracování zaznamenána v Záznamech zpracování OÚ.

4.10 Likvidace osobních údajů

Garant zpracování OÚ je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti Subjektu údajů. Další podmínky obsahují směrnice Organizace s názvem Archivační a skartační řád, případně Spisový a skartační plán.

4.11 Předávání údajů do jiných států

OO, která hodlá předávat osobní údaje do zahraničí, sdělí tuto skutečnost DPO.

DPO neprodleně OO informuje o tom, zda je možné osobní údaje předat do zahraničí nebo o podmínkách, které musí být splněny, aby mohlo k předání dojít.

4.12 Odpovědnost

Zodpovědnosti DPO, GZOÚ, ředitele a OO jsou uvedeny v kapitole Matice odpovědnosti.

Všichni zaměstnanci jsou povinni zejména:

a) dodržovat pravidla stanovená touto směrnicí, úkoly a pokyny GZOÚ a DPO, zejména pak zpracovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny a v rozsahu nezbytném pro naplnění stanoveného účelu,

b) zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních k jejich ochraně; povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo příslušných prací,

c) v případě zjištění neoprávněného nakládání s osobními údaji informovat bezodkladně DPO.

4.13 Technická a bezpečnostní opatření k zajištění ochrany osobních údajů

Organizace je povinna přijmout technicko-organizační opatření k zajištění ochrany osobních údajů.

Technicko-organizačními opatřeními zejména jsou:

1. personální opatření
2. administrativní opatření
3. opatření fyzické ochrany
4. opatření pro ochranu OÚ v ICT
5. opatření při bezpečnostních incidentech

4.13.1. Personální opatření

Jedná se o opatření, která se týkají zaměstnanců Organizace, smluvních partnerů a dalších osob, které se podílejí nebo přicházejí do styku s osobními údaji, které zpracovává Organizace. Tyto osoby musí být prokazatelné seznámeny s pravidly při nakládání s osobními údaji, a to formou školení, prokazatelným prohlášením obsahujícím závazek mlčenlivosti, úpravou popisu pracovního místa a pracovní náplně, schválením přístupů nadřízeným zaměstnancem, na základě uzavřené smlouvy atp.

Zaměstnanci Organizace jsou povinni se zúčastnit školení o postupech ochrany osobních údajů v rozsahu potřebném k výkonu svých funkcí. Školení zajišťuje DPO.

4.13.2. Administrativní opatření

V rámci přijatých opatření k ochraně osobních údajů jsou posuzována rizika týkající se:

a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům;

b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování;

c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje;

d) funkčnosti opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

Posouzení rizik provádí DPO minimálně 1x za kalendářní pololetí. O provedeném posouzení je sepsán zápis, včetně návrhu opatření ke snížení rizik.

Na základě analýzy rizik musí být stanovena procesní opatření, kterými jsou vázáni zaměstnanci Organizace. Jedná se zejména o postupy, jak zacházet s osobními údaji, jak klasifikovat a označovat osobní údaje, řídit záznamy v souladu se spisovým a skartačním řádem, ukládání osobních údajů, archivace a skartace atp.

Na základě těchto procesů a postupů jsou všichni zaměstnanci Organizace, manipulující s osobními údaji, povinni tyto údaje chránit.

Dále sem patří i opatření pro kontrolu a dohled nad zpracováním osobních údajů, kterou provádí DPO.

Kontrola je prováděna minimálně 1x za kalendářní pololetí. O provedené kontrole musí být proveden záznam, kde bude uvedena doba kontroly, zjištěný stav, případně opatření k odstranění zjištěných nedostatků.

Na základě zjištěných nedostatků při kontrolní činnosti DPO, nebo po obdržení upozornění na nedostatky ze strany DPO, ředitel přijme odpovídající opatření k odstranění zjištěných nedostatků.

4.13.3. Opatření fyzické ochrany

Fyzickou bezpečnost tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k osobním údajům nebo jiným utajovaným informacím Organizace. Pokud

opatření nejsou schopná přímo zabránit, tak mají dále za cíl alespoň bezpečnostní incident zaznamenat.

Fyzické zabezpečení je zpravidla zajišťováno kombinací opatření, jako je ostraha, režimová opatření a technické prostředky. Rozsah fyzické bezpečnosti musí určit Organizace na základě analýzy možných rizik.

Mezi zabezpečení fyzické ochrany patří:

- mechanické zábranné prostředky,
- elektrická zámková zařízení a systémy pro kontrolu vstupů (čipové karty apod.),
- zařízení elektrické zabezpečovací signalizace (pohybová čidla, magnetická čidla, kamerové systémy),
- skartovací zařízení pro ničení papírových záznamů s osobními údaji,
- zařízení fyzického ničení elektronických nosičů dat.

4.13.4. Opatření pro ochranu OÚ v ICT

Veškeré nosiče osobních údajů musí být mechanicky, nebo elektronicky zabezpečeny proti neoprávněnému použití nebo poškození. Data na nosičích osobních údajů musí být šifrována, přístup musí být řízený a musí být o něm prováděny záznamy (logy).

Nosiče s osobními údaji je možné uchovávat pouze v uzamykatelných místnostech. Nosiče osobních údajů, které obsahují citlivé údaje, je možné uchovávat pouze v uzamykatelných skříních umístěných v uzamykatelných místnostech.

Elektronické nosiče osobních údajů, je možné uchovávat v počítači či podobném zařízení pouze:

a) je-li přístup k takovýmto souborům chráněn heslem, a zároveň

b) je-li přístup do HW zařízení chráněn heslem.

U automatizovaného informačního systému je nutné:

- zajištění bezporuchového a nepřerušeného provozu zařízení výpočetní techniky,
- dodržování zásad bezpečného používání počítačových systémů,
- kontrola a zabezpečení přístupu k počítačovým systémům,
- zajištění ochrany nosičů osobních údajů,
- zajištění zálohování a obnovy dat a SW vybavení počítačových systémů,
- používání antivirové ochrany.

4.13.5. Opatření při bezpečnostních incidentech

Při zjištění neoprávněného nakládání s osobními údaji, jakož i při zjištění jiných porušení povinností stanovených GDPR, musí být stanovena opatření, kdy je osoba, která toto porušení zjistí, povinna neprodleně informovat DPO a GZOÚ.

Zpracovávané osobní údaje jsou v případě potřeby vydávány správním orgánům a orgánům činným v trestním řízení pro účely řízení o přestupku nebo správního deliktu a

trestního řízení na základě jejich odůvodněné písemné žádosti na základě záznamu o vydávání osobních údajů oprávněným zaměstnancem.

Škola se při své činnosti řídí především následujícími právními předpisy:

▪ *zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů*

▪ *vyhláška č. 48/2004 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky, ve znění pozdějších předpisů*

▪ *vyhláška č. 74/2005 Sb., o zájmovém vzdělávání, ve znění pozdějších předpisů*

▪ *vyhláška č. 27/2016 Sb., o vzdělávání žáků se speciálními vzdělávacími potřebami a žáků nadaných, ve znění pozdějších předpisů*

Škola přijímá žádost o informace v listinné nebo elektronické podobě. Součástí přijetí žádosti je ověření totožnosti žadatele z důvodu ochrany jeho osobních údajů.

Způsob ověření totožnosti:

- *Přijetí žádosti datovou schránkou z datové schránky subjektu údajů.*
- *Přijetí žádosti prostřednictvím e-mailu s platným kvalifikovaným elektronickým podpisem.*
- *Ověřením totožnosti na podatelně MČ Praha 8 při podání žádosti.*
- *Listinná žádost je podepsána ověřeným podpisem.*

Jiný způsob ověření není přípustný.

Poskytnutí informace je bezplatné. V případě, že požadavek na poskytnutí informací bude zjevně bezdůvodný nebo nepřiměřený, zejména opakovaný v krátké době, je možné požadovat úhradu přiměřených nákladů. Zjevně bezdůvodný nebo nepřiměřený požadavek je možné odmítnout.

5. Závěrečná ustanovení

Tato směrnice nabývá účinnosti 25.5.2018.

Za seznámení všech zaměstnanců s touto směrnicí zodpovídá ředitel Školy.