Směrnice
Pravidla pro ochranu osobních údajů

Účinnost: 2.9.2024
Počet stran: 26
Počet příloh: 4
Rozdělovník: dostupné v Internetu, v ředitelně školy
Kód normy: GDPR
Ruší: Směrnici o ochraně osobních údajů z 1. 9. 2021

Článek 1
Účel a rozsah působnosti

1.1 Tato směrnice stanovuje práva a povinnosti při zpracování a ochraně osobních údajů, a upravuje procesní organizační opatření k zajištění povinností vyplývajících z legislativního rámce pro ochranu osobních údajů.

1.2 Směrnice se vydává v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

1.3 Směrnice upravuje povinnosti Organizace a jejích zaměstnanců při provádění automatizovaného zpracování osobních údajů a při provádění neautomatizovaného zpracování těch osobních údajů, které jsou Organizací zpracovávány. Směrnice se nevztahuje na nahodilé, neúmyslné získání osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

1.4 Organizace je v postavení Správce osobních údajů a z tohoto důvodu je zodpovědná za zpracování získávaných údajů v souladu s platnou legislativou. Organizace se zavazuje shromažďovat a vést pouze takové osobní údaje o subjektech, které umožňují poskytovat bezpečné, odborné a kvalitní služby. Pro práci s těmito osobními údaji byl vytvořen příslušný systém práce pro všechny personální úrovně, byl definován soubor osobních údajů, jejichž získávání je pro zajištění poskytování kvalitních, odborných a bezpečných služeb klientům nezbytné, dále bylo přesně vymezeno, k jakému účelu budou konkrétní osobní údaje využívány a také byla posouzena možná rizika spojená se zajištěním bezpečnosti osobních údajů a jejich správou. V organizačním a pracovním řádu byly ustanoveny role/pozice odpovědné za dodržování legislativní podmínek v oblasti ochrany osobních údajů.

1.5 Tato směrnice je závazná pro všechny zaměstnance Denního a týdenního stacionáře Jihlava, příspěvková organizace, kteří přichází do styku s osobními údaji.

Článek 2
Použité zkratky a zástupná označení

Zkratka	Popis
DPIA	Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)
IP adresa	Jednoznačná identifikace zařízení v počítačové síti
Pověřenec	Pověřenec pro ochranu osobních údajů
Legislativní rámec	Zákon č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů, Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Zákon č. 89/2012 Občanský zákoník,
MAC	Jednoznačný identifikátor síťového zařízení (tzv. fyzická adresa)
Obecné nařízení	Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních

	údajů a o volném pohybu těchto údajů
Garant agendy	Osoba odpovědná za agendu zpracování osobních údajů (vedoucí odborných útvarů / sekcí apod.)
ÚIT	(IT oddělení, odpovědný za zajištění informační bezpečnosti)
OÚ	Osobní údaje
Provoz	(oddělení technické správy, odpovědný za zajištění fyzické bezpečnosti)
Organizace	Denní a týdenní stacionář Jihlava, příspěvková organizace
ZOÚ	Zaměstnanec odpovědný za ochranu osobních údajů v Organizaci

Článek 3
Výklad pojmů

3.1 **Osobní údaje** - 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.

Konkrétní osobu lze identifikovat zejména různou kombinací osobních údajů.

Příklad osobních údajů resp. údajů pro kombinace osobních údajů vyskytující se obvykle v Organizaci:

- Jméno
- Příjmení
- Podpis
- Datum a místo narození
- Rodné číslo
- Pohlaví
- Trvalé bydliště
- Soukromé telefonní číslo
- Firemní telefonní číslo
- Soukromý email
- Firemní email
- Číslo občanského průkazu
- Číslo pasu
- Číslo řidičského průkazu
- Certifikát pro elektronický podpis
- Údaje v osobní evidenci
- Údaje v mzdové evidenci
- Údaje pro zdravotní pojišťovnu
- Údaje pro splnění kvalifikačních předpokladů
- Životopis
- Záznam o dopravní nehodě služebního vozidla
- Kamerové záznamy, fotografie
- IP adresy, MAC adresy

3.2 **Zvláštní kategorie osobních údajů** - je osobní údaj, který vypovídá o národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách a hnutích, nebo odborových či zaměstnaneckých organizacích, náboženství a filosofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů.
Příklady zvláštní kategorie osobních údajů obvykle se vyskytujících v Organizaci:

- Údaje o příslušnosti k odborové organizaci (srážky ze mzdy - příspěvky)

3.3 **Subjekt údajů** - fyzická osoba, kterou lze přímo či nepřímo identifikovat pomocí osobních údajů.

3.4 **Správce** - Škola - právnická osoba, která určuje účely a prostředky zpracování osobních údajů.

3.5 **Zpracovatel** – fyzická (OSVČ) nebo právnická osoba, která zpracovává osobní údaje pro Správce.

3.6 **Likvidace osobních údajů** - je fyzické zničení nosiče osobních údajů, jejich fyzické vymazání nebo trvalé vyloučení z dalšího zpracování.

3.7 **Zpracování** - 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.

3.8 **Profilování** - jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

3.9 **Porušení 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.

3.10 **Dozorový úřad** - Úřad pro ochranu osobních údajů.

3.11 **Dokument** – fyzický (papírový) dokument, nebo el. datový soubor obsahující osobní údaje

3.12 **Kopie dokumentu** – scan, fotokopie (apod.) fyzického dokumentu, anebo datová kopie el. souboru

3.13 **Zabezpečené úložiště** - datový prostor jako je centrální diskové pole, pevný disk počítačů, spisový uzel, spisovna.

3.14 **Evidence úložišť OÚ** - evidence všech úložišť, kde je možné ukládat OÚ, např.:

a) centrální datové úložiště a informační systémy
b) pevný disk osobního počítače
c) přenosné úložiště (flash disk, externí pevný disk)
d) úložiště přenosných zařízení (notebook, tablet, telefon)
e) úložiště fyzických dokumentů (spisové uzly, spisovny)

3.15 **Datové inventurní záznamy** - obsahují informace o jednotlivých zpracování OÚ ve Škole v rozsahu nezbytném pro generování záznamů o zpracování, vytváření podkladů pro rizikovou analýzu a podkladů pro rozhodování o nutnosti provedení DPIA.

3.16 **Evidence porušení zabezpečení OÚ** – obsahuje dokumentaci veškerých případů porušení zabezpečení osobních údajů, přičemž jsou uvedeny skutečnosti, které se týkají daných porušení, jejich účinky a přijatá nápravná opatření.

3.17 **Evidence požadavků subjektů údajů** - obsahuje záznamy o požadavcích subjektů údajů na přístup k OÚ, opravu OÚ, výmaz OÚ, omezení zpracování a vznesení námitky včetně informace o tom, jak byly tyto požadavky vypořádány.

Část I.
Vybrané obecné podmínky pro zpracování OÚ

Článek 4
Zásady zpracování osobních údajů

4.1 OÚ 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 („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 („omezené 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“)

Článek 5
Zákonnost zpracování

5.1 Zpracování OÚ je zákonné, pokud je splněna alespoň jedna z těchto podmínek:

a) subjekt údajů udělil souhlas se zpracováním svých OÚ pro jeden či více konkrétních účelů *(čl. 6, odst. 1. a) Obecného nařízení)*,

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 *(čl. 6, odst. 1. b) Obecného nařízení)*,

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje *(čl. 6, odst. 1. c) Obecného nařízení)*,

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby *(čl. 6, odst. 1. d) Obecného nařízení)*,

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce *(čl. 6, odst. 1. e) Obecného nařízení)*,

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce 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 *(čl. 6, odst. 1. f) Obecného nařízení)*.

5.2 Zakazuje se zpracování zvláštní kategorie OÚ, pokud nejde o jeden z níže uvedených případů:

a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů *(čl. 9, odst. 2. a) Obecného nařízení)*,

b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany *(čl. 9, odst. 2. b) Obecného nařízení)*,

c) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů *(čl. 9, odst. 2. e) Obecného nařízení)*,

d) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického významu nebo pro statistické účely, které je přiměřené sledovanému cíli, dodržuje podstatu práva na OÚ a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů *(čl. 9, odst. 2. j) Obecného nařízení)*.

Článek 6
Souhlas se zpracováním osobních údajů

6.1 Souhlas musí být svobodným, konkrétním (pro konkrétní účel zpracování), informovaným a jednoznačným projevem vůle subjektu údajů, který jím dává své svolení ke zpracování svých osobních údajů.

6.2 Subjekt údajů musí být před udělením souhlasu informován o všech skutečnostech zpracování, zejména o Organizaci jako správci, účelech zpracování, o operacích zpracování a o možnosti kdykoli odvolat souhlas, nikoli však se zpětnými účinky.

6.3 Souhlas musí být udělen v písemné formě, a to buď v listinné, nebo v elektronické podobě.

6.4 Pokud je od Subjektu údajů nutné získat Souhlas se zpracováním, musí se tak stát za pomoci samostatného dokumentu (v listinné, nebo elektronické podobě).

6.5 Subjekt údajů je oprávněn jím udělený souhlas kdykoli odvolat. Odvolat souhlas musí být stejně snadné jako jej poskytnout. V případě, že Organizaci bude doručeno odvolání souhlasu je Organizace povinna postupovat v souladu s postupy uvedenými v této směrnici.

6.6 V případě, že subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování, Organizace je povinna provést likvidaci osobních údajů, které se daného subjektu údajů týkají.

6.7 Organizace eviduje informace o uděleném souhlasu v následujícím rozsahu: kdo a kdy souhlas udělil, rozsah informací poskytnutých subjektu údajů před udělením souhlasu a forma udělení souhlasu. Součástí evidence je též žádost o vyjádření souhlasu, pokud byla předložena subjektu údajů, a záznam o uděleném souhlasu. V případě, že subjekt údajů souhlas odvolal, je součástí evidence též údaj o odvolání souhlasu a o datu odvolání souhlasu.

6.8 Udělený souhlas je platný pouze pro operace zpracování, které jsou nezbytné a přiměřené k naplnění účelu, pro který byl souhlas udělen.

6.9 Souhlas se zpracováním osobních údajů dítěte mladšího 13/16 let je platný pouze v případě, že je vyjádřen nebo schválen jeho zákonným zástupcem.

Článek 7
Zpracování zvláštních osobních údajů

7.1 Organizace smí zpracovávat zvláštní osobní údaje pouze v případech, kdy jde o některý z případů vymezených ve čl. 9 odst. 2 nařízení GDPR, zejména

a) subjekt údajů udělil výslovný souhlas se zpracováním zvláštních osobních údajů pro jeden či více konkrétních účelů, nebo
b) zpracování je nezbytné pro účely plnění povinností vyplývajících ze smlouvy mezi subjektem a Organizací.

Oprávněný zájem Organizace

7.2 Organizace je oprávněna zpracovávat osobní údaje subjektu údajů v případě, je-li zpracování nezbytné pro účely plnění oprávněných zájmů Organizace či třetí osoby.

7.3 Oprávněným zájem Organizace může být např. zveřejňování osobních údajů v rámci práva na informace, přímý marketing a profilování, ochrana před zneužitím služeb, ochrana majetkových zájmů, zajištění bezpečnosti sítě a informací a z dalších důvodů.

7.4 V každém jednotlivém případě, kdy má dojít ke zpracování osobních údajů na základě oprávněného zájmu, je nutné stanovit oprávněný zájem a dále posoudit:

a) oprávněnost stanoveného zájmu, tedy zda je stanovený zájem legální a dostatečně specifický a zda jde o skutečný zájem Organizace,
b) nezbytnost zamýšleného zpracování osobních údajů pro účely stanoveného zájmu, zda je v rovnováze oprávněný zájem Organizace a práva subjektu údajů
c) zda nad stanoveným zájmem Organizace nepřevažují zájmy nebo základní práva a svobody subjektu údajů, včetně posouzení případného přijetí záruk k ochraně práv a svobod subjektů údajů.

7.5 V případě, že jsou splněny všechny výše uvedené požadavky, smí být v rámci Organizace zahájeno zpracování osobních údajů z důvodu oprávněného zájmu.

Článek 8
Záznamy o činnostech zpracování

8.1 Každý správce vede Záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace:

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu OÚ,
b) účely zpracování,
c) popis kategorií subjektů údajů a kategorií osobních údajů,
d) kategorie příjemců OÚ, kterým byli nebo budou OÚ zpřístupněny,
e) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
f) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

8.2 Záznamy se vyhotovují písemně, v to počítaje i elektronickou formu.

8.3 Pro každý účel zpracování OÚ v Organizaci musí být vypracován a veden záznam o činnosti zpracování viz Příloha č. 3.

8.4 Za věcnou správnost jednotlivých záznamů o činnostech zpracování je odpovědný příslušný garant agendy, v jehož organizačním útvaru probíhá zpracování OÚ, při současném zohlednění zásad zpracování OÚ dle článku 4 této směrnice.

8.5 Evidenci všech záznamů o činnostech zpracování v Organizaci vede ZOÚ.

8.6 ZOÚ zajišťuje, aby Záznamy o činnostech zpracování byly k dispozici v aktuální formě (elektronické a písemné, nebo jen písemné).

8.7 Kontrola a aktualizace jednotlivých záznamů o činnostech zpracování se provádí 1x ročně. ZOÚ vyzve odpovědné garanty agendy zasláním příslušných evidovaných záznamů k ověření jejich správnosti, aktuálnosti a případnému doplnění, včetně stanovení příslušných lhůt pro provedení kontroly.

Článek 9
Posouzení vlivu na ochranu osobních údajů (DPIA)

9.1 Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním DPIA.

9.2 DPIA je nutné zejména v těchto případech:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,

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

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Článek 10
Zabezpečení zpracování

10.1 S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování OÚ,

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,

c) schopnosti obnovit dostupnost OÚ a přístup k nim včas v případě fyzických či technických incidentů,

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

10.2 Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných OÚ, nebo neoprávněný přístup k nim.

10.3 Zpracovat a evidovat přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů v souladu s nařízením a zvláštními a interními předpisy.

10.4 Zajistit, že užívat systémy pro automatizované zpracování osobních údajů mohou pouze oprávněné osoby, a to pouze v rozsahu odpovídajícímu jejich oprávnění,

10.5 Zajistit elektronické záznamy o přístupu k osobním údajům a provedených úkonech i zpracování osobních údajů.

10.6 Zabránit neoprávněnému přístupu k nosičům informací.

10.7 Posoudit, zda bude docházet k předání osobních údajů třetím osobám a zda jsou splněny všechny podmínky předání v souladu s nařízením a touto směrnicí.

Článek 11
Uzavírání smluv se zpracovateli OÚ

11.1 Pro zpracování OÚ využije Správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Obecného nařízení a aby byla zajištěna dostatečná ochrana práv subjektu údajů.

11.2 Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího písemného povolení Správce.

11.3 Zpracování zpracovatelem se řídí smlouvou, která zavazuje Zpracovatele vůči Správci a v níž je stanoven předmět a doba trvání, povaha a účel zpracování, typ OÚ a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt stanoví zejména, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce,
b) zajišťuje, aby se osoby oprávněné zpracovávat OÚ zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
c) zajistí zabezpečení zpracování zejména:
   - pseudonymizace a šifrování OÚ,
   - schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
   - schopnost obnovit dostupnost údajů a přístup k nim v případě fyzických či technických incidentů,
   - proces pravidelného testování, posuzování a hodnocení účinnosti zavedených opatření.
d) je nápomocen při zajištění souladu s následujícími povinnostmi:
   - zabezpečení zpracování,
   - ohlašování případů porušení zabezpečení OÚ dozorovému úřadu,
   - oznamování případů porušení zabezpečení OÚ subjektu údajů,
   - posouzení vlivu na ochranu OÚ,
   - předchozí konzultace (před zpracováním s dozorovým úřadem),
   - v souladu s rozhodnutím správce všechny OÚ buď vymaže, anebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním a vymaže existující kopie, pokud legislativa nepožaduje uložení daných OÚ,
   - poskytne správci veškeré informace potřebné k doložení toho, že byly splněny všechny povinnosti a umožní audity včetně inspekcí prováděné správcem nebo jiným auditorem, kterého správce pověřil.

Článek 12
Právo subjektu údajů na přístup k OÚ

12.1 Subjekt údajů má právo získat od správce potvrzení, zda OÚ, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto OÚ a k následujícím informacím:

a) účely zpracování,
b) kategorie dotčených OÚ,
c) příjemci nebo kategorie příjemců, kterým byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích,
d) plánovaná doba, po kterou budou OÚ uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,

e) existence práva požadovat od správce opravu nebo výmaz OÚ 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 OÚ, pokud nejsou získány od subjektu údajů,
h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a informace týkající se použitého postupu.

12.2 Správce poskytne kopii zpracovávaných OÚ zdarma. Za další kopie na žádost subjektu údajů může správce 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.

12.3 Právem získat kopii nesmí být dotčena práva a svobody jiných osob.

Článek 13
Právo subjektu na opravu

13.1 Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné OÚ, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných OÚ, a to i poskytnutím dodatečného prohlášení.

Článek 14
Právo subjektu na výmaz („právo být zapomenut“)

14.1 Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal OÚ, které se daného subjektu údajů týkají, a správce má povinnost OÚ bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:
a) OÚ 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,
c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, nebo subjekt údajů vznese námitky proti zpracování v případech zpracování pro účely přímého marketingu,
d) OÚ byly zpracovány protiprávně,
e) OÚ byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

Článek 15
Právo subjektu na omezení zpracování

15.1 Subjekt údajů má právo na to, aby správce omezil zpracování v kterémkoli z těchto případů:
a) subjekt údajů popírá přesnost OÚ, a to na dobu potřebnou k tomu, aby správce mohl přesnost OÚ ověřit,
b) zpracování je protiprávní a subjekt údajů odmítá výmaz OÚ a žádá místo toho o omezení jejich použití,

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, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Článek 16
Právo na podání námitky

16.1 Subjekt údajů má právo kdykoliv vnést námitku proti zpracování osobních údajů.

Článek 17
Právo na přenositelnost údajů

17.1 Subjekt údajů má právo získat OÚ, které se ho týkají, jež poskytl Správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a právo předat tyto údaje jinému Správci, a to v případě že:
a) zpracování je založeno na souhlasu se zpracováním osobních údajů *(čl. 6, odst. 1. a) Obecného nařízení)* nebo na souhlasu se zpracováním zvláštní kategorie osobních údajů *(čl. 9, odst. 2 a) Obecného nařízení)* nebo na smlouvě *(čl. 6, odst. 1. a) Obecného nařízení)*,
b) zpracování se provádí automatizovaně.

17.2 Subjekt údajů má právo na to, aby OÚ byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

17.3 Tímto právem nesmí být nepříznivě dotčena práva a svobody jiných osob.

Článek 18
Ohlašování případů porušení zabezpečení OÚ

18.1 Jakékoli porušení zabezpečení OÚ Správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, 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.

18.2 Ohlášení dozorovému úřadu musí obsahovat:
a) popis povahy daného případu porušení zabezpečení OÚ včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů OÚ,
b) kontaktní místo, které může poskytnout bližší informace,
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

18.3 Správce dokumentuje veškeré případy porušení zabezpečení OÚ, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí být na vyžádání přístupná dozorovému úřadu.

18.4 Pokud je pravděpodobné, že určitý případ porušení zabezpečení OÚ bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Správce toto porušení bez zbytečného odkladu subjektu údajů.

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

a) Správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u OÚ dotčených porušením zabezpečení OÚ, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup, jako je např. šifrování,

b) Správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů se již pravděpodobně neprojeví,

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

Část II.
Aplikace podmínek pro zpracování OÚ v Organizaci

Článek 19
Zpracování osobních údajů v rámci Organizace

19.1 V rámci Organizace je povoleno zpracovávat osobní údaje pouze za podmínek stanovených nařízením a touto směrnicí.

19.2 V rámci lidských zdrojů je možné zpracovávat osobní údaje o zaměstnancích stanovené zvláštními zákony (např. zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů, zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů, apod.), a to pro účely pracovněprávního vztahu a pro plnění úkolů uložených zákonem č. 262/2006 Sb., zákoníkem práce, ve znění pozdějších předpisů, nebo zvláštním právním předpisem, po dobu nezbytnou k zajištění práv a povinností, plynoucích z tohoto pracovněprávního nebo jiného obdobného vztahu.

19.3 Při vstupu osob, které nejsou v pracovněprávním vztahu nebo v jiném obdobném vztahu k Organizaci, do jejích prostor, jež nejsou určeny pro veřejnost, je požadováno jméno a příjmení, druh a číslo dokladu totožnosti. Uvedené údaje jsou zpracovávány pro účely oprávněných zájmů Organizace. Mohou být zpracovány bez souhlasu subjektu údajů.

19.4 Organizace zpracovává kontaktní údaje osob ze smluv.

Článek 20
Povinnosti při zpracování OÚ

Pro zpracování OÚ v Organizaci platí následující povinnosti a pravidla:

20.1 Všichni zaměstnanci jsou povinni zachovávat mlčenlivost o veškerých informacích, se kterými byli obeznámeni v souvislosti se zpracováním OÚ. Povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo příslušných prací. Mlčenlivost se vztahuje i na opatření, která slouží k zabezpečení zpracování OÚ.

20.2 Zaměstnanci nesmí umožnit nahlížet do OÚ či předávat OÚ neoprávněným osobám.

20.3 Zaměstnancům je zakázáno bezdůvodně pořizovat kopie nebo videozáznamy (fotografie) OÚ, ani pořizovat kopie souborů obsahující OÚ.

20.4 U kopie dokumentu obsahující OÚ je potřeba uplatňovat stejná pravidla pro ochranu OÚ jako u originálu.

20.5 Zaměstnanci, kteří si pořídili kopii dokumentu obsahující OÚ výhradně pro pracovní potřebu, tuto kopii po skončení důvodu pro zpracování skartují či v případě elektronické kopie odstraní.

20.6 Všem zaměstnancům je zakázáno OÚ ukládat na vnitřních i externích paměťových médiích osobních počítačů a mobilních zařízeních. Výjimky schvaluje příslušný garant agendy. Adekvátní zajištění úložiště OÚ (např. šifrování), zajistí ÚIT a ohlásí k zaevidování ZOÚ do seznamu úložišť.

20.7 Všem zaměstnancům je zakázáno zpracovávat OÚ na neschválených IT prostředcích.

20.8 Je zakázáno posílat dokumenty obsahující OÚ e-mailem mimo interní síť. V případě potřeby předání OÚ mimo interní síť Organizace, musí být přenos přiměřeně zajištěn, např. šifrováním dokumentu, anebo použitím zabezpečeného kanálu.

20.9 Všichni garanti agend v Organizaci, v jejichž útvaru se pracuje s OÚ/jsou odpovědni za zpracování OÚ, jsou povinni přijmout takové opatření (v případě technických opatření ve spolupráci s příslušnými organizačními jednotkami), aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k OÚ, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití. Tato povinnost platí i po ukončení zpracování OÚ.

Článek 21
Evidence přijatých technických a organizačních opatření

21.1 Organizační a technická opatření:

- **Personální bezpečnost**
  - S osobními údaji je oprávněna se seznámit pouze oprávněná osoba, a to v rozsahu odpovídajícímu jejímu oprávnění. Oprávnění této osoby vyplývá z její pracovní náplně na základě uzavřeného pracovněprávního vztahu nebo obdobného vztahu. Oprávněná osoba musí mít objektivní a důvodnou potřebu seznámit se s osobními údaji za účelem plnění pracovních povinností či jiných povinností nebo oprávněných zájmů.
- **Fyzická bezpečnost**
  - Dokumenty s osobními údaji se ukládají na příslušných pracovištích (kanceláře, archivy apod.) v souladu se Spisovým řádem a ostatními interními předpisy.
  - Dokumenty musí být ukládány v uzamčených schránkách (kancelářské skříně, trezorové skříně, plechové skříně, stolní kontejnery apod.), bez možnosti přístupu neoprávněných osob v mimopracovní době i v době krátkodobé nepřítomnosti (oběd, přestávka apod.).
  - Klíči od uzamčené schránky disponuje vlastník procesů nebo jím určená osoba. Duplikáty klíčů od uzamčené schránky jsou uloženy u přímého nadřízeného vlastníka procesů nebo jím určené osoby v zapečetěné obálce.

- V době nepřítomnosti vlastníka procesu může uzamčenou schránku bez souhlasu vlastníka procesu otevřít pouze nejblíže nadřízený zaměstnanec vlastníka procesu nebo jím určená osoba.
- Při skončení pracovněprávního vztahu vlastníka procesu zabezpečí předání údajů jiné osobě nejblíže nadřízený zaměstnanec vlastníka procesu. Pokud není přebírající znám, vlastník informace předá dokumenty nejblíže nadřízenému zaměstnanci, nebo dokumenty uloží do spisovny Organizace v zabezpečeném obalu, ke kterému přiloží seznam ukládaných dokumentů.

- **Informační bezpečnost osobních údajů ukládaných v ICT Organizace**
  - Zabezpečení přístupu k osobním údajům zpracovávaných v ICT Organizace vychází ze směrnic uvedených v připojené tabulce, které jsou v souladu s doporučením řady norem ISO/IEC 27000.
  - Osobní údaje nesmí být zasílány mimo datovou síť Organizace a pokud možno ani v rámci datové sítě Organizace v nezašifrované podoby.

Článek 22
Nové zpracování OÚ, změna stávajícího zpracování OÚ

22.1 Nové zpracování, či změnu stávajícího zpracování OÚ zajišťuje odpovědný garant agendy při současném zohlednění zásad zpracování OÚ dle článku 4 této směrnice.

22.2 V případě nového zpracování či změny stávajícího zpracování OÚ je příslušný garant agendy povinen vypracovat, či aktualizovat příslušný Datový inventurní záznam (v případě technických opatření ve spolupráci s příslušnými organizačními jednotkami – ÚIT, Provoz aj.), a odeslat jej k vyjádření ZOÚ.

22.3 Na základě nového, či aktualizovaného Datového inventurního záznamu provede ZOÚ vyhodnocení nutnosti DPIA, a v případě potřeby zajistí jeho realizaci.

22.4 DPO zajistí ve spolupráci s garantem agendy, ÚIT a Provozem analýzu rizik (případně aktualizaci) dopadu konkrétního zpracování na subjekty osobních údajů.

Článek 23
Likvidace osobních údajů

23.1 Po ukončení zpracování OÚ, nebo na základě oprávněné žádosti subjektu OÚ zajistí likvidaci OÚ příslušný garant agendy.

23.2 Při likvidaci těchto údajů je nutné vyplnit Likvidační protokol (viz Příloha č. 3), který musí být podepsán 2 oprávněnými zaměstnanci, které určí příslušný garant agendy. Protokoly o likvidaci OÚ eviduje odpovědný garant agendy nebo jím pověřený pracovník.

23.3 Dokumenty musí být likvidovány v souladu s interním předpisem Spisový a skartační řád.

23.4 Likvidaci fyzických dokumentů zajišťuje příslušný pracovník (oprávněný pracovník za účasti druhého oprávněného pracovníka) skartováním.

23.5 Vymazání OÚ z úložišť a systémů zajišťuje ÚIT.

Článek 24
Evidence úložišť OÚ

24.1 Evidenci úložišť OÚ v Organizaci vede ZOÚ.

24.2 Zabezpečení datových úložišť OÚ, např. dle bodu 3.14, písm. a) a b), zajišťuje ÚIT.

24.3 Zabezpečení přenosných úložišť OÚ, např. dle bodu 3.14, písm. c) a d), zajišťuje příslušný zaměstnanec, kterému byly přiděleny.

24.4 Zabezpečení fyzických úložišť OÚ, např. dle bodu 3.14, písm. e), zajišťuje Provoz.

24.5 V případě změny nebo aktualizace zabezpečení úložišť zašle ÚIT nebo Provoz požadavek na změnu, resp. aktualizaci k vyjádření ZOÚ a k provedení aktualizace Evidence úložišť.

24.6 ZOÚ následně ve spolupráci s příslušným garantem agendy provede aktualizaci Datových inventurních záznamů.

Článek 25
Postupy Správce při výkonu práv subjektu údajů

25.1 Subjekt údajů je oprávněn žádat o:

a) Přístup k OÚ
b) Opravu OÚ
c) Výmaz OÚ
d) Omezení zpracování, vznést námitku

25.2 Subjekt údajů za účelem výkonu svých práv může podat žádost osobně, písemně či v elektronické formě (prostřednictvím datové schránky, zveřejněné e-mailové schránky).

25.3 Organizace předá informaci či jinak vyřídí žádost subjektu údajů ve formě preferované subjektem údajů. Pokud ji subjekt údajů nezvolil, platí, že odpověď a další komunikace probíhá ve formě odpovídající podané žádosti. V případě, že subjekt údajů podal žádost v elektronické formě, Organizace poskytne informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.

25.4 Po převzetí žádosti odpovědná osoba v Organizaci (definovaná v organizační struktuře organizace či dle pracovní pozice jako osoba odpovědná za oblast bezpečnosti ochrany osobních údajů, pokud tomu tak není pak samotné vedení Organizace) žádost zaeviduje a zahájí její vyřízení.

25.5 Organizace je jako Správce povinna ověřit totožnost žadatele a určit, zda se skutečně jedná o oprávněný subjekt údajů. Pokud žádost neobsahuje dostatek údajů k tomu, aby Organizace mohla žadatele či subjekt údajů bezpečně identifikovat, vyzve žadatele, aby svou žádost doplnil dodatečnými informacemi nezbytnými k potvrzení totožnosti subjektu údajů a případnými informacemi o službách, které využívá. V případě, že ani po tomto doplnění nebude možné subjekt údajů identifikovat, pak Organizace informuje o této skutečnosti žadatele a výkon práva neumožní.

25.6 Organizace je povinna podle náležitostí přijaté žádosti bez zbytečného odkladu, a vždy do jednoho měsíce od obdržení žádosti poskytnout žadateli/subjektu údajů informace o přijatých krocích. Lhůtu jednoho měsíce je možné o další dva měsíce prodloužit s ohledem na složitost a počet žádostí přijatých během období jednoho měsíce od přijetí žádosti. V prodloužené lhůtě nelze žádost odmítnout. Organizace musí informovat žadatele/ subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

25.7 Pokud Organizace žádost odmítne, bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti informuje žadatele/subjekt údajů o důvodech odmítnutí a o možnosti podat stížnost u úřadu a žádat o soudní ochranu.

25.8 Organizace poskytuje informace v rámci výkonu práv subjektu údajů bezplatně.

25.9 V případě, že Organizace žádost vyhodnotí jako zjevně nedůvodnou nebo nepřiměřenou, má právo žádost odmítnout nebo vyřízení žádosti zpoplatnit. Organizace před vyměřením přiměřeného poplatku informuje žadatele o jeho výši a požádá jej o souhlas.

25.10 Organizace je povinna oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy, likvidaci osobních údajů nebo omezení zpracování s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí.

25.11 ZOÚ s pomocí ÚIT, případně s příslušným garantem agendy:

a) V případě žádosti o přístup k OÚ:
   - zajistí informaci, zda jsou o dotyčném subjektu zpracovávány OÚ,
   - informuje subjekt o zpracovávaných údajích v rozsahu Záznamu o zpracování,
   - pokud to subjekt požaduje, poskytne buď fyzickou, nebo elektronickou kopii zpracovávaných OÚ.

b) V případě žádosti o opravu:
   - ověří a aktualizuje příslušné OÚ v souladu s požadavkem subjektu,

- informuje subjekt o provedení aktualizace osobních údajů.

c) V případě žádosti o výmaz:
- rozhodne, zda je žádost o výmaz oprávněná a pokud ano, zajistí výmaz předmětných OÚ,
- informuje subjekt o výmazu příslušných OÚ, případně o nemožnosti výmaz provést, a to včetně odůvodnění nemožnosti.

d) V případě vznesení námitky či žádosti o omezení zpracování:
- rozhodne, zda je žádost na omezení zpracování oprávněná a pokud ano, zajistí pozastavení zpracování předmětných OÚ. Pokud není oprávněná, informuje o této skutečnosti neprodleně subjektu údajů,
- informuje subjekt o pozastavení či následné obnově pozastaveného zpracování.

e) V případě požadavku na přenositelnost OÚ:
- rozhodne, zda je žádost přenositelnost OÚ oprávněná a pokud ano, zajistí OÚ ve strukturovaném, běžně používaném a strojově čitelném formátu,
- předá OÚ ve strukturovaném, běžně používaném a strojově čitelném formátu subjektu údajů nebo přímo novému správci, je-li to technicky proveditelné.

25.12 V případě obnovy dat ze záloh zajistí ÚIT na základě Evidence požadavků subjektu OÚ prověření a opětovné smazání příslušných OÚ dříve, než budou systému uvolněny zpět do produkčního provozu.

Článek 26
Hlášení porušení zabezpečení OÚ

26.1 Zaměstnanec, který zjistí porušení zabezpečení osobních údajů, nahlásí tuto skutečnost neprodleně ZOÚ.

26.2 ZOÚ informuje příslušného garanta agendy o porušení zabezpečení OÚ, případně další organizační jednotky (např. ředitele).

26.3 ZOÚ vyhodnotí pravděpodobnost rizika porušení zabezpečení pro práva a svobody fyzických osob a v souladu s ustanoveními článku 14 ohlásí dozorovému úřadu, v případě vysokého rizika pro práva a svobody fyzických osob i subjektu údajů.

26.4 ZOÚ dokumentuje veškeré případy porušení zabezpečení osobních údajů v Evidenci porušení zabezpečení OÚ, přičemž uvede skutečnosti, které se týkají daného porušení, jeho dopady a přijatá nápravná opatření. Tato dokumentace musí být na vyžádání přístupná dozorovému úřadu.

26.5 Garant agendy, odpovědný za zpracování příslušných OÚ zajistí ve spolupráci s ZOÚ, a příslušnými organizačními jednotkami nápravná opatření a provede případné změny v Datovém inventurním záznamu.

Článek 27
Hlášení porušení zabezpečení OÚ dozorovému orgánu

27.1 Pověřená osoba zahájí ve spolupráci dotčenými útvary interní vyšetřování. Pokud ze závěru interního vyšetřování vyplývá, že k porušení zabezpečení osobních údajů došlo a je zde riziko pro práva a povinnosti fyzických osob, ohlásí pověřená osoba/pověřenec tuto skutečnost bez zbytečného odkladu úřadu.

27.2 Ohlášení musí být doručeno úřadu bez zbytečného odkladu, nejpozději do 72 hodin od zjištění skutečnosti, která s vysokou pravděpodobností představuje porušení zabezpečení osobních údajů. Pokud do této lhůty není ohlášení úřadu doručeno, musí být zároveň s ohlášením uvedeny relevantní důvody tohoto zpoždění.

27.3 Ohlášení dle odst. musí mít písemnou formu a musí obsahovat:

a) Popis povahy daného porušení zabezpečení osobních údajů. Pokud je to možné včetně kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného počtu dotčených záznamů subjektů údajů.

b) Jméno a kontaktní údaje pověřené osoby/ pověřence.

c) Popis pravděpodobných důsledků, které porušení zabezpečení osobních údajů představuje.

d) Popis nápravných opatření, která byla přijata nebo navržena k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

e) Organizace oznámí bez zbytečného odkladu po ukončení interního vyšetřování dle kapitoly subjektu údajů porušení zabezpečení osobních údajů, pokud toto porušení bylo v závěru interního vyšetřování vyhodnoceno jako vysoce rizikové pro práva a povinnosti fyzických osob.

f) Oznámení není nutné činit v případě, že:

- byla zavedena náležitá technická a organizační opatření a tato 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 (např. šifrování),
- byla přijata nápravná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví,
- podání oznámení vyžaduje nepřiměřené úsilí. V takovém případě musí být subjekt údajů informován stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Článek 28
Uzavření smlouvy se zpracovateli OÚ

28.1 Přípravu smlouvy se zpracovatelem OÚ zajišťuje příslušný garant agendy ve spolupráci s příslušnými odbornými útvary Organizace a ZOÚ. Smlouva musí respektovat Článek 11 této směrnice.

28.2 ZOÚ ověřuje zapracování požadavků Článek 11 do smlouvy.

Článek 29
Pověřenec pro ochranu osobních údajů

29.1 Organizace stanoví, kdo a jakým způsobem zajišťuje roli Pověřence.

29.2 Pověřenec je zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů v Organizaci.

29.3 Pověřenec není odpovědný za nedodržení pravidel stanovených nařízením a touto směrnicí při postupech oblasti osobních údajů.

29.4 Je zakázáno uložit pověřenci pokyny týkající se výkonu jeho úkolů.

29.5 Pověřenec je vázán povinností mlčenlivosti ohledně skutečností, které se dozvěděl při výkonu své funkce, a to i po skončení smluvního či pracovněprávního vztahu.

29.6 Vedení organizace oznámí vhodným způsobem úřadu, veřejnosti a všem zaměstnancům kontaktní údaje pověřence.

29.7 Subjekty údajů se mohou obracet na pověřence ve všech záležitostech souvisejících se zpracováním osobních údajů a výkonem jejich práv. Žádosti a stížnosti subjektů údajů budou vyřízeny a stížnosti dle této směrnice.

29.8 Pověřenec nesmí při své činnosti určovat účely nebo prostředky zpracování osobních údajů.

29.9 Pověřenec se nesmí dostat do situace, kdy by sám kontroloval své vlastní postupy.

Článek 30
Vzdělávání

30.1 ZOÚ zajistí pravidelné vzdělávání zaměstnanců, kteří přichází do styku s osobními údaji.

Článek 31
Odpovědnost a povinnosti Správce při zpracování osobních údajů

31.1 Organizace jako Správce odpovídá za dodržování jednotlivých povinností stanovených právními předpisy upravujícími ochranu osobních údajů.

31.2 Organizace má definované role a odpovědnosti při zpracování osobních údajů v rámci své působnosti (ustanovené v organizačním/pracovním řádem a pracovními náplněmi).

31.3 Organizace vystupuje převážně v roli Správce.

31.4 Zmocnění ke zpracování osobních údajů vyplývá ze zvláštního právního předpisu nebo ze smlouvy o zpracování osobních údajů, případně z uděleného Souhlasu od subjektu. Ve všech případech musí být dostatečným způsobem upraveny požadavky na vhodná technická a organizační opatření na ochranu osobních údajů.

31.5 Pokud se na zpracování osobních údajů v gesci Správce podílí třetí strana (Zpracovatel), pak Organizace smí využít pouze takového Zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky stanovené nařízením a touto směrnicí a aby byla zajištěna ochrana práv subjektů. Smlouva o zpracování osobních údajů Zpracovatelem musí mít písemnou formu. Ve smlouvě musí být uveden předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva Správce, požadavky na vhodná technická a organizační opatření na ochranu osobních údajů, resp. záruky Zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů, jež má dle smlouvy zpracovat, a požadavky na poskytování součinnosti při ohlašování případů porušení zabezpečení osobních údajů úřadu. Smlouva musí obsahovat i další náležitosti stanovené v čl. 28 odst. 3 nařízení.

31.6 Organizace v pozici Správce určuje účely a prostředky zpracování osobních údajů a nese za tuto činnost odpovědnost. Jestliže Organizace zjistí, že Zpracovatel porušuje povinnosti stanovené nařízením, je povinna na tuto skutečnost Zpracovatele neprodleně upozornit a ukončit zpracování osobních údajů Zpracovatelem.

31.7 Organizace jako Správce nebo Zpracovatel spolupracuje na požádání s úřadem při plnění jeho úkolů

Článek 32
Závěrečná ustanovení

32.1 Všichni vedoucí pracovníci jsou povinni prokazatelně (proti podpisu) seznámit s touto směrnicí zaměstnance jimi řízeného útvaru, kteří přicházejí do styku s osobními údaji.

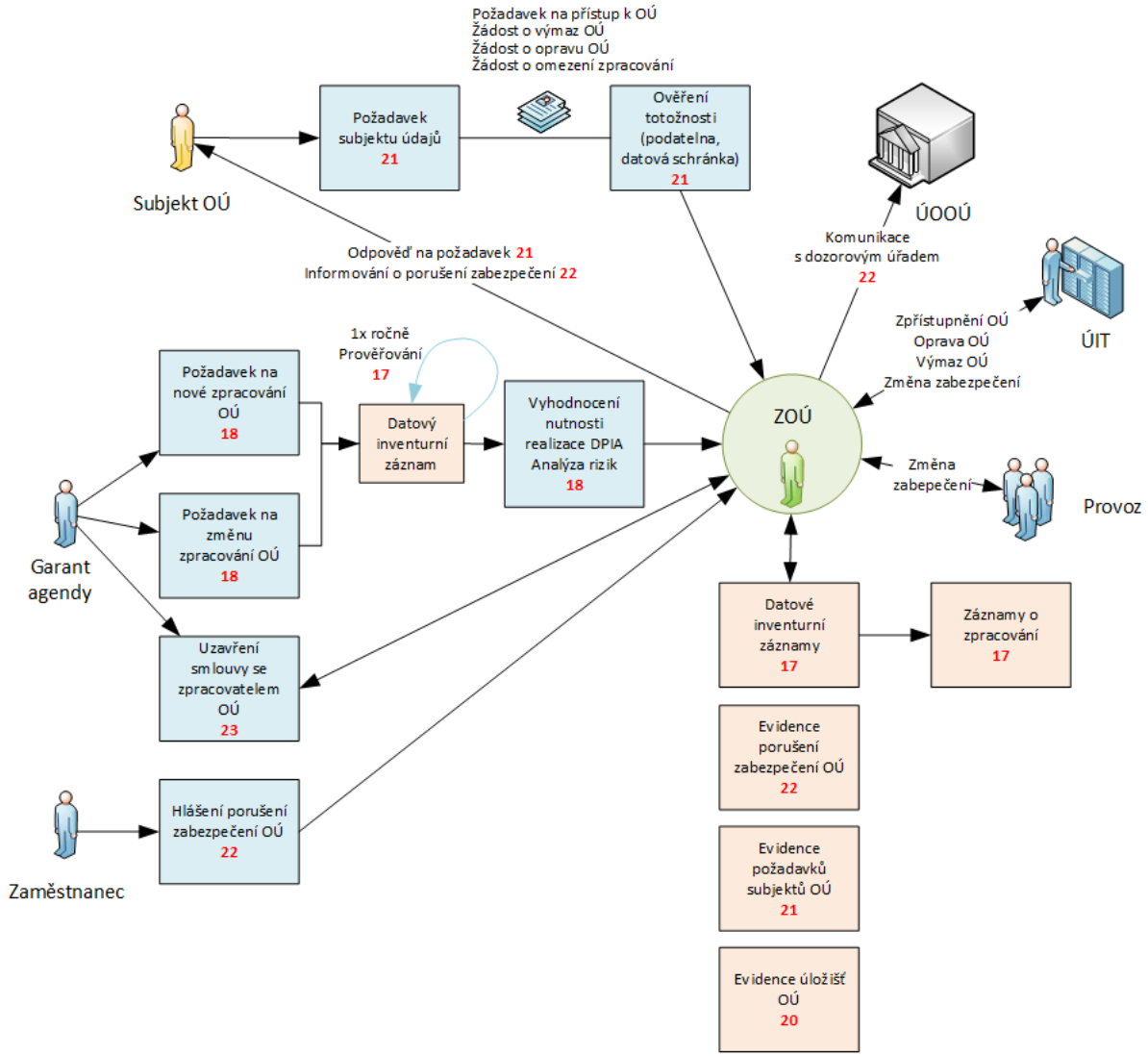
32.2 Tato směrnice nabývá platnosti dne 2. 9. 2024

32.3 Odborný výklad k této směrnici podá ZOÚ.

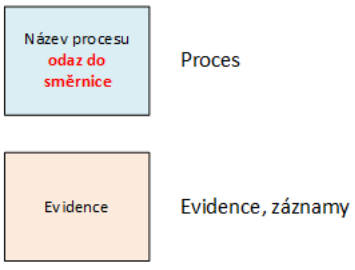
Přílohy:

Příloha č. 1 – Postupy pro zpracování a ochranu osobních údajů v Organizaci
Příloha č. 2 – Likvidační protokol
Příloha č. 3 – Záznam o činnostech zpracování
Příloha č. 4 – Přístupová práva k OÚ v rámci organizace

Příloha č. 1 - Postupy pro zpracování a ochranu osobních údajů v Organizaci



Legenda



Příloha č. 2 – Likvidační protokol

LIKVIDAČNÍ PROTOKOL

1. Útvar likvidující osobní údaje: ……

2. Název materiálu obsahujícího osobní údaje (pokud se jedná o více subjektů údajů, uvést výčet v příloze k protokolu):

……..

……..

……..

……..

3. Způsob likvidace:

……..

……..

……..

4. Místo likvidace:

……..

……..

5. Datum likvidace (popř. údaj o době, po které je likvidace prováděna):

……..

6. Jméno a podpis vedoucího, který schválil likvidaci:

……..

7. Jméno a podpisy dvou zaměstnanců určených vedoucím útvaru, kteří odpovídají za provedení likvidace:

…… ……

Příloha č. 3 – Záznam o činnostech zpracování

Záznam o činnostech zpracování *

Záznam o činnostech zpracování

Informace o správci

Jméno správce	
Kontaktní údaje správce	Tel: Email:
Kontaktní údaje pověřence pro ochranu osobních údajů	Email:

Identifikace zpracování

Oblast	
Popis zpracovaných OÚ	
Poznámka	
Role organizace	
Účely zpracování	
Kategorie subjektů údajů	
Kategorie OÚ	
Zpracovávané OÚ	
Kategorie příjemců OÚ	
Příjemci OÚ mimo EU	
Lhůta pro výmaz	
Zpracovatelé OÚ	

Popis technických bezpečnostních opatření pro elektronická data

Informační systémy/služby				
Informační systém				
Outsourcing (služba)				
Šifrování mimo interní síť				
Logování čtení				
Pseudonimizace				
Oprávnění OU				
Podpora výmazu OÚ				
Řízen přístup k zálohovacím médiím				
Podpora omezení zpracování OÚ				
Archivace mimo systém				
Logování změn				
Systematické zálohování				
Zálohy šifrovány				
Řízení přístupu				

Popis technických bezpečnostních opatření pro fyzické dokumenty

Názvy fyzických dokumentů		
Spisové uzly, kde se dokument vyskytuje v rámci zpracování		
Cílové spisové uzly, kde je dokument ukládán před archivací ve spisovně		
Uzel		
Druhý zámek		
Vrátnice		
Klíče		
Uzamykatelná registratura		
EZS		
Vstupní karta		
Přístup veřejnosti do uzlu		

Organizační bezpečnostní opatření

* Dle Článku 30 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.4.2016

Příloha č. 4 – Přístupová práva k OÚ v rámci organizace

Stanovení oprávnění a přehled osob, které mají právo přístupu k osobním údajům v Organizaci

	Stanovení oprávnění a přehled osob, které oprávněním přístupu k citlivým osobním údajům v Organizaci disponují	Smlouvy	Osobní údaje zaměstnanců	Další evidence Organizace
1.	Ředitel	☺	☺	☺
2.	Zástupce ředitele	☺	☺	
3.	Ekonomka a personalistka školy	☺	☺	☺
4.	Administrativní pracovnice	☺	☺	☺
5.	ICT koordinátor			☺
6.	Další…….			