Směrnice
o nakládání s osobními údaji

Městská knihovna Most,
příspěvková organizace

Účinnost od 01. 05. 2026

Zpracovatel:

Ředitel Městské knihovny Most, příspěvkové organizace

Článek 1

Úvodní ustanovení

Tato Směrnice o nakládání s osobními údaji (dále jen směrnice) se vydává v souladu s ust. § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění a je vnitřním předpisem (dále jen „příspěvková organizace“ nebo „PO“), který specifikuje ustanovení 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), někdy také General Data Protection Regulation (dále jen „Nařízení GDPR“), případně dalších souvisejících předpisů a je závazný pro všechny zaměstnance PO.

Článek 2

Předmět, účel a působnost

1) Směrnice stanovuje taková opatření a pravidla, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných MK Most, PO. Ochranou osobních údajů je míněno zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich integrity, dostupnosti a dalších bezpečnostních aspektů všech osobních údajů v míře potřebné pro činnost PO, a to v souladu s Nařízením GDPR a jinými právními předpisy.

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

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

   - Organizační řád Městské knihovny Most, příspěvkové organizace,
   - Knihovní řád Městské knihovny Most, příspěvkové organizace
   - Spisový řád a skartační plán Městské knihovny Most, příspěvkové organizace,

   a s touto směrnicí.

4) Systém ochrany osobních údajů definovaný touto směrnicí je navržen a zpracován v souladu s Nařízením GDPR.

5) Přehled spravovaných datových sad osobních údajů formou Záznamů o činnostech zpracování je zaměstnancům PO k dispozici ve složce GDPR v kanceláři ředitele č. 147. Zpracování Záznamů o činnostech zpracování bylo provedeno dialogem s odpovědnými pracovníky PO. Záznamy o činnostech zpracování jsou pravidelně aktualizovány.

6) Směrnice je závazná pro všechny osoby organizačně zařazené do struktury PO (zaměstnanci PO, včetně DPP, DPČ, praktikanti, dobrovolníci a brigádníci).

7) Osoby, které osobní údaje zpracovávají v roli zpracovatele na základě smlouvy uzavřené s PO jakožto správcem osobních údajů jsou k dodržování ochrany osobních údajů zavázáni uzavřením smlouvy o ochraně osobních údajů podle článku 24 této směrnice.

Článek 3

Pojmy a definice

Pro účely této směrnice se rozumí:

1) „**osobními údaji**“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „**subjekt údajů**“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

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

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

4) „**zpracováním**“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo

pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

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

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

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

8) „**správcem**“ PO jako orgán veřejné moci, které sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;

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

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

11) „**souhlasem**“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

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

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

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

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

16) „**Unií**“ Evropská unie;

17) **„členské státy“** Členské státy Evropské unie;

18) „**zaměstnancem**“ fyzická osoba, která měla nebo má pracovně-právní vztah s PO;

19) **„třetí země“** země mimo Evropskou unii.

20) **„pověřenec pro ochranu osobních údajů“** (dále už jen „Pověřenec“) osoba, jmenovaná statutárním zástupcem k monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z Nařízení GDPR, provádění interních auditů, školení zaměstnanců, komunikaci se subjekty údajů a Dozorovým úřadem a řízení agendy ochrany osobních údajů.

Článek 4

Rozsah působnosti

1) Ředitel odpovídá za to, že jemu podřízení zaměstnanci, kteří nakládají s osobními údaji a vystupují v roli uživatelů nebo správců osobních údajů, byli seznámeni s pravidly ochrany osobních údajů, tj. s touto směrnicí. Zaměstnanci PO jsou povinni dodržovat pravidla pro nakládání s osobními údaji.

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

Článek 5

Určení rolí v systému ochrany osobních údajů

1) Ředitel příspěvkové organizace

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

- schvaluje Směrnici o nakládání s osobními údaji a její aktualizace;
- jmenuje Pověřence pro ochranu osobních údajů v případě, kdy Pověřenec není jmenován zřizovatelem;
- projednává pravidelnou zprávu o stavu ochrany osobních údajů PO;
- rozhoduje o přijetí technických, fyzických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR a dalšími platnými právními předpisy na ochranu osobních údajů;
- zajišťuje, aby každý zaměstnanec PO před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen a proškolen se zásadami ochrany osobních údajů a touto směrnicí a zajišťuje v roční frekvenci prokazatelné opakování tohoto proškolení;

- zajišťuje, aby každý zaměstnanec PO před prvním přístupem ke spravovaným osobním údajům písemně potvrdil Prohlášení o ochraně osobních údajů;
- při uzavírání smluv s třetími stranami dbát na to, aby obsahovaly zásady zajištění ochrany osobních údajů, pokud je to vzhledem k povaze obsahu smlouvy relevantní.

2) Pověřenec pro ochranu osobních údajů

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

- poskytování informací a poradenství zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů;
- monitorování souladu s touto směrnicí, Nařízením GDPR a dalšími předpisy Unie nebo členských států v oblasti ochrany osobních údajů a s vnitřními předpisy PO v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
- zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji PO;
- zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci v rámci PO;
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR;
- spolupráce s dozorovým úřadem;
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci;
- působení jako kontaktní místo pro subjekty údajů. Subjekty údajů se mohou obracet na Pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Nařízení GDPR.

Pověřenec má neomezený přístup k centrální evidenci zpracování osobních údajů a kontroluje její pravidelnou aktualizaci zodpovědnými osobami.

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

Pověřenec pro ochranu osobních údajů je přímo podřízen řediteli PO.

Pověřenec pro ochranu osobních údajů nedostává žádné pokyny týkající se výkonu svých úkolů (ředitel PO nemůže Pověřenci zadat pokyn, jakého výsledku má dosáhnout nebo jaký

názor nebo právní výklad má zastávat, jak prošetřit stížnost a námitku nebo zda kontaktovat dozorový úřad).

V souvislosti s plněním svých úkolů nesmí být Pověřenec propuštěn ani sankcionován. Pověřence nelze nijak postihovat za nezávislý způsob výkonu povinností (tzn. za to, že zastává jiný názor než správce osobních údajů, nebo že kontaktoval dozorový úřad atp.), např. ukončením smlouvy o spolupráci, snížením odměny za výkon funkce pověřence nebo jakýmkoli jiným způsobem.

Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí, a to v souladu s právem Unie nebo zákony a právními předpisy České republiky. Pověřenec může plnit i jiné úkoly a povinnosti, které však nesmějí vést ke střetu zájmů jeho činností.

3) Uživatelé osobních údajů

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

- dodržovat zásady vyplývající z této směrnice a související dokumentace;
- hlásit veškeré bezpečnostní incidenty svému nadřízenému, případně přímo Koordinátorovi;
- informovat Koordinátora a ředitele PO o zjištěných bezpečnostních slabinách;
- informovat Koordinátora a ředitele PO o změnách ve způsobu zpracování a nakládání s osobními údaji;
- vykonávat další činnosti vyplývající z platných vnitřních předpisů PO, především zajistit průběh skartačního řízení v souladu se Spisovým a skartačním řádem PO.

4) Administrátoři

Administrátoři jsou zaměstnanci PO nebo externí administrátoři, kteří mají na starost provoz a údržbu systémů a aplikací, zálohování a zabezpečení (elektronických) dat uživatelů, a pracovníci odpovědní za řízení a implementaci bezpečnosti systémů. Administrátoři mají obvykle přístup ke všem datům uloženým v informačním systému PO nebo fyzický přístup k zařízením, pomocí nichž jsou tato data zpracovávána. S externím administrátorem musí být vždy sepsána smlouva o mlčenlivosti.

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

Článek 6

Přístup k osobním údajům

K osobním údajům mají přístup pouze ředitel, Uživatelé osobních údajů, Koordinátor, Pověřenec a Administrátoři.

Článek 7

Zásady zpracování osobních údajů

1) Osobní údaje musí být:

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

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

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

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

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

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

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

3) Písemnosti obsahující osobní údaje podléhají procesu fyzické a elektronické skartace v souladu se Spisovým a skartačním řádem PO. V případě neevidovaných dokumentů (dokumentace na vědomí, kopie písemností a dalších dokumentů bez čísla jednacího) je za jejich likvidaci v elektronické i fyzické podobě odpovědný Uživatel osobních údajů.

4) Pro statistické účely je nutné osobní údaje anonymizovat.

5) Je třeba zamezit neoprávněnému přístupu ke shromážděným údajům.

Článek 8

Zákonnost zpracování osobních údajů

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

   a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
   b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
   c) zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na PO jako správce osobních údajů;
   d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
   e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřena PO jako správce osobních údajů;
   f) zpracování je nezbytné pro účely oprávněných zájmů PO jako správce osobních údajů či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. Toto se netýká zpracování prováděného PO jako správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.

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

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

a) souhlas musí být udělen samostatně a musí být jasně odlišitelný od ostatních sdělení (jako samostatný dokument). Vzor souhlasu se zpracováním osobních údajů je zaměstnancům PO k dispozici ve složce GDPR v kanceláři ředitele č. 147,

b) souhlas může udělit subjekt údajů nebo jeho zákonný zástupce, pokud je subjektu údajů dítě;

c) subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu, včetně informace o způsobu odvolání uděleného souhlasu;

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

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

f) subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně dostupné jako jej poskytnout;

g) v případě využití konkludentního souhlasu[1] je nutné zajistit informování subjektu údajů (Informační memorandum na webových stránkách PO, informační tabule u vstupu na akce, informace na přihlášce, pozvánce, na webovém formuláři a dalších místech sběru osobních údajů);

h) uživatel osobních údajů je povinen ve spolupráci s ředitelem PO zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat. V případě technických problémů ředitel PO zkonzultuje postup s Administrátorem.

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

Článek 9

Opatření pro ochranu a zabezpečení osobních údajů

1) Uživatel osobních údajů je povinen dodržovat pravidlo čistého stolu (neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole, po ukončení pracovního dne je každý zaměstnanec povinen takové listinné písemnosti uložit do

[1] Konkludentní právní jednání je projev vůle učiněný jiným způsobem než slovně (tedy ne ústně nebo písemně), přičemž právně jednající takovým způsobem, jako je např. kývnutí hlavou, potřesení rukou, nevyjádření protestu, mlčky, vyjádří svou vůli se právně vázat.

uzamykatelných úložných prostor a klíče zajistit tak, aby k nim neměly přístup osoby bez oprávnění).

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

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

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

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

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

7) Uživatel osobních údajů není oprávněn ukládat písemnosti obsahující osobní údaje na sdílené disky PO, pokud to nevyžaduje spolupráce více Uživatelů a přístup na sdílené disky je omezen pouze na skupinu spolupracujících oprávněných Uživatelů osobních údajů PO.

8) Uživatel osobních údajů je povinen využívat pro ukládání fyzické dokumentace obsahující osobní údaje (včetně fyzických nosičů elektronické dokumentace) k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění kanceláře uzamknout. Uživatel osobních údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat skartační znaky dle platného Spisového a skartačního řádu PO. To platí i pro písemnosti na vědomí, kopie písemností a další dokumenty bez čísla jednacího.

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

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

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

12) Uživatel osobních údajů není oprávněn přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé e-mailové schránky (např. www.seznam.cz, www.gmail.com apod.) nezabezpečeným způsobem (pokud zákon neukládá jinak, např. zákon 106/1999 Sb.).

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

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

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

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

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

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

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

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

Článek 10

Předávání osobních údajů

1) Dokumentaci obsahující osobní údaje v elektronické podobě je povoleno předávat příjemcům mimo PO pouze prostřednictvím datových schránek. V případech, kdy není možné dokumentaci předat prostřednictvím datové schránky nebo ve fyzické podobě, lze dokumentaci předat zabezpečeným způsobem (tj. např. v podobě šifrovaného souboru ve formátu zip a heslo k odšifrování předat příjemcům nezávislým kanálem, např. zasláním na mobilní telefon).

2) Předávání osobních údajů v analogové podobě zabezpečeně v přepravním kontejneru nebo doporučenou poštou.

Článek 11

Zveřejňování osobních údajů

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

2) Musí dojít k zajištění anonymizace osobních údajů uvedených v uzavřených smlouvách, které jsou zveřejněny v Registru smluv a na dalších místech.

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

4) V případě pořizování fotografické nebo video dokumentace z veřejných akcí PO, musí PO zajistit informování účastníků o pořizování této dokumentace za účelem informování veřejnosti o činnosti PO a možném uložení do odvolání uděleného souhlasu. Pracovníci pořizující tuto dokumentaci musí být viditelně výrazně označeni.

5) Fotografie zaměstnanců PO se mohou zveřejňovat na webových stránkách PO apod., pouze po výslovném souhlasu zaměstnance PO s tímto zveřejněním (souhlas není vynutitelný) s výjimkou případů uvedených v odstavci 4.

Článek 12

Získávání informací od subjektu údajů

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

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

2) Naplnění informační povinnosti podle bodu 1) může být zajištěno zveřejněním Informačního memoranda na webových stránkách PO.

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

Článek 13

Práva subjektu údajů

1) Subjekt údajů může uplatnit tato práva:

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

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

3) Subjektu údajů (v případě nezletilého jeho zákonnému zástupci) jsou poskytovány informace především stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků,

4) Informace jsou subjektu údajů (v případě nezletilého jeho zákonnému zástupci) poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (občanský průkaz, datová schránka).

5) Postup naplnění práv subjektů údajů definuje Metodika pro plnění povinností vůči Subjektům údajů PO.

Článek 14

Právo subjektu údajů na přístup k osobním údajům

1) Subjekt údajů má právo získat od PO jako správce osobních údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

   a) účely zpracování;
   b) kategorie dotčených osobních údajů;

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

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

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

f) právo podat stížnost u dozorového úřadu;

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

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

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

Článek 15

Oprava a výmaz osobních údajů

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

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

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování a jejich uchovávání;

c) subjekt údajů vznese námitky proti zpracování s ohledem na uplynutí lhůty pro zpracování nebo s ohledem na prokazatelnou nedostatečnost zabezpečení osobních údajů;

d) osobní údaje byly zpracovány protiprávně;

e) osobní údaje musí být skartovány ke splnění právní povinnosti stanovené právem Unie nebo zákony a platnými právními předpisy České republiky, které se na PO jako správce osobních údajů vztahují.

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

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

a) pro výkon práva na svobodu projevu a informace;

b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo ČR, které se na PO jako správce osobních údajů vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je PO pověřena;

c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2) písm. h) a i) a čl. 9 odst. 3) Nařízení GDPR;

d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle zvláštních právních předpisů;

e) pro určení, výkon nebo obhajobu právních nároků.

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

Článek 16

Právo na omezení zpracování

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

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

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

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

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

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

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

Článek 17

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

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

2) Naplnění informační povinnosti podle bodu 1) může být zajištěno zveřejněním Informačního memoranda na webových stránkách PO.

Článek 18

Právo na přenositelnost údajů

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

   a) zpracování je založeno na uděleném souhlasu se zpracováním osobních údajů nebo na uzavřené smlouvě;
   b) zpracování se provádí v elektronické podobě.

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

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

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

Článek 19

Právo vznést námitku

1) Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají. PO jako správce osobních údajů osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

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

Článek 20

Řešení případů porušení zabezpečení osobních údajů

1) Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec neprodleně řediteli PO a současně přímo Pověřenci pro ochranu osobních údajů a zřizovateli prostřednictvím svodného odboru.

2) Okamžité hlášení bude obsahovat minimálně tyto informace:

   a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
   b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů pro PO jako správce osobních údajů a pro subjekty údajů;
   c) návrh okamžitých opatření k zastavení porušení zabezpečení osobních údajů a případně návrh okamžitých nápravných opatření.

3) Pověřenec pro ochranu osobních údajů ve spolupráci s ředitelem PO, Uživateli osobních údajů, Administrátory, relevantními zpracovateli osobních údajů, případně dalšími relevantními zaměstnanci PO, rozhodne o dalším postupu.

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

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

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

Článek 21

Činnost při zjištění porušení zabezpečení osobních údajů

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

2) Ředitel organizace spolupracuje při řízení reakce na incident s orgány veřejné správy.

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

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

5) Hlavními cíli řízení reakce na incident jsou:

   a) ověřit, zda skutečně došlo k porušení zabezpečení osobních údajů;
   b) zjistit, zda došlo k neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů, případně jinému nežádoucímu stavu nebo dopadu;
   c) zamezit možnosti neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů;
   d) zjistit rozsah incidentu;
   e) zjistit, které osoby se mohly neoprávněně s osobními údaji seznámit;
   f) zjistit, kde se osobní údaje a informační systémy nacházejí v rozporu s předpisy PO a obecně závaznými právními normami;
   g) opatřit důkazy pro řízení, vyšetřování nebo dokazování. Pokud je to třeba, použijí se forenzní metody a standardy;

h) zjistit, zda je potřebné oznamovat incident třetím stranám;

i) navrhnout a přijmout taková opatření, aby incident pominul;

j) navrhnout a přijmout taková opatření, aby se incident neopakoval;

k) sdílet nebo předat varování třetím osobám, zejména zřizovateli příspěvkové organizace a dozorovému úřadu tak, aby se předešlo incidentům u dalších správců.

6) Činnost podle tohoto článku se ukončí, jestliže o tom rozhodne ředitel organizace na základě zprávy zpracované Pověřencem a zabezpečených podkladů a informací, nebo pokud se prokáže, že k incidentu nedošlo. Pokud se prokáže, že k incidentu nedošlo, vypracuje Pověřenec zprávu v obdobném rozsahu.

7) Zprávu předkládá ředitel organizace na vědomí zřizovateli prostřednictvím svodného odboru.

8) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu Pověřenci a řediteli organizace.

Článek 22

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1) Jakékoli porušení zabezpečení osobních údajů Pověřenec za PO 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.

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

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

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

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

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

3) Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Pověřenec pro ochranu osobních údajů dokumentuje veškeré případy

porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Článek 23

Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

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

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

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

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

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

Článek 24

Zpracovatel

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

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

3) Zpracování zpracovatelem se řídí smlouvou. Ředitel PO je povinen zajistit, aby s každým zpracovatelem byla před zahájením zpracování uzavřena Smlouva o zpracování osobních údajů, která zavazuje zpracovatele vůči PO jako správci osobních údajů a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.

Článek 25

Kontrola dodržování ustanovení směrnice

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

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

3) K seznámení s pravidly o nakládání s osobními údaji je směrnice přístupná též ostatním uživatelům počítačové sítě PO.

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

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

Článek 26

Revize směrnice

1) Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.
2) Za zpracování, prosazení, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá ředitel PO.

Článek 27

Platnost a účinnost směrnice

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

V Mostě dne 01. 05. 2026

Bc. Petr Petrik
Ředitel PO

Příloha č. 1 – Používání nástrojů umělé inteligence (AI)

1. Zásady práce s AI

Nástroje umělé inteligence (dále jen „AI“) se používají pouze způsobem, který je v souladu s touto směrnicí, obecně závaznými právními předpisy a zásadami zpracování osobních údajů. AI slouží jako podpůrný nástroj; nenahrazuje odborný úsudek zaměstnanců organizace ani jejich odpovědnost.

2. Zákaz vkládání osobních údajů do externích AI nástrojů

Není-li v této směrnici výslovně stanoveno jinak, je zakázáno zadávat do externích AI nástrojů jakékoli osobní údaje subjektů údajů, se kterými organizace v rámci své činnosti pracuje (zejména klientů, dětí a jejich zákonných zástupců, zaměstnanců, dodavatelů a dalších fyzických osob), a to zejména:

- jména a příjmení, kontaktní údaje a identifikátory, včetně rodného čísla, čísla dokladu totožnosti (občanského průkazu / pasu), čísla pojištěnce, interních evidenčních čísel (spisová značka, číslo jednací, klientský / pacientský identifikátor), uživatelských účtů a dalších jedinečných identifikátorů;
- údaje o přestupcích, opatřeních, sankcích a souvisejících řízeních;
- jakékoli další údaje, které by samostatně nebo ve spojení s dalšími informacemi mohly umožnit přímou či nepřímou identifikaci konkrétní osoby (např. pracovní zařazení, lokalita, fotografie apod.).

3. Výjimky a bezpečné prostředí

Má-li být AI nástroj použit způsobem, při němž může docházet ke zpracování osobních údajů, je takové použití přípustné pouze při splnění všech níže uvedených podmínek:

- je využito výhradně takové prostředí, které je předem schváleno ředitelem podle postupu popsaného ve Směrnici o využívání umělé inteligence.
- musí být vyhodnocen právní základ zpracování, proporcionalita a rizika pro práva subjektů údajů; je-li to přiměřené povaze a rozsahu zpracování, provede se posouzení vlivu na ochranu osobních údajů (DPIA).

4. Automatizované rozhodování

Není povoleno používat výstupy AI k plně automatizovanému rozhodování tj. k rozhodování bez lidského zásahu, které by mělo právní účinky vůči subjektům údajů nebo se jich obdobně významně dotýkalo nebo o jiných úředních či správních úkonech s dopadem na fyzické osoby).

AI může být použita pouze jako podklad pro rozhodnutí, které vždy činí konkrétní odpovědný zaměstnanec organizace.

5. Kontrola a odpovědnost zaměstnanců

Každý zaměstnanec, který použije AI, je povinen výstupy AI přiměřeně zkontrolovat a kriticky posoudit. Výstupy AI mohou obsahovat nepřesné, neúplné nebo smyšlené informace a nesmí být považovány za samostatný nebo primární zdroj faktických či právních informací.

Využití nesprávných nebo nepřesných výstupů vygenerovaných AI nezbavuje zaměstnance odpovědnosti za případnou škodu způsobenou organizaci nebo třetím osobám.

Zaměstnanci jsou povinni používat AI nástroje pouze v rozsahu, pro který byli proškoleni, a v souladu s pravidly organizace pro bezpečné a odpovědné využívání AI.

6. Logy a evidence

Při systematickém zpracování osobních údajů prostřednictvím schváleného AI nástroje se vede přiměřená evidence použití (např. logy o přístupech, základní technické záznamy) v rozsahu nezbytném pro prokázání souladu s GDPR, pro šetření incidentů a výkon práv subjektů údajů. Doba uchování těchto záznamů se řídí spisovým a skartačním řádem organizace.

7. Informování subjektů údajů a transparentnost použití AI

Subjekty údajů musí být přiměřeným způsobem informovány o zpracování jejich osobních údajů v souladu s čl. 7 GDPR a Směrnicí o využívání umělé inteligence.

Jsou-li výstupy AI využity jako podklad pro rozhodování nebo posuzování týkající se konkrétních fyzických osob, musí být tato skutečnost výslovně uvedena v informacích poskytovaných subjektům údajů a na žádost se poskytne stručný a srozumitelný popis role AI v daném procesu, včetně toho, jaký lidský dohled a kontrola byly uplatněny.

V Mostě dne 1. 5. 2026

Bc. Petr Petrik

ředitel MKM