Směrnice o nakládání s osobními údaji

Centrum sociálních a zdravotních služeb města Příbram, p. o.
Se sídlem: Brodská 100, Příbram VIII, 261 01
IČ 47067071

(dále jen **Správce OÚ**)

Platnost od 1.8.2020
Revize první s platností od 1.4.2024

I.
Úvodní ustanovení

1. Tato Směrnice o nakládání a zpracování s osobními údaji (dále jen tato směrnice a/nebo směrnice) se vydává na základě 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).

II.
Předmět, účel a působnost

1. Směrnice stanovuje opatření a pravidla, která zabraňují neoprávněnému nebo nahodilému přístupu k osobním údajům, a dále jejich změně, zničení či ztrátě, neoprávněným přenosům, jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných Správcem OÚ. Ochranou osobních údajů dle směrnice se rozumí zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich správnosti, integrity, dostupnosti a splnění dalších bezpečnostních a jiných požadavků v případě všech osobních údajů v míře potřebné pro činnost Správce OÚ, a to v souladu se zákonem a jinými právními předpisy.
2. Tato směrnice se zabývá ochranou všech osobních údajů ve vlastnictví, ve správě Správce OÚ nebo Správcem OÚ zpracovávaných, 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 Správce OÚ ustanoven systém řízení ochrany osobních údajů, který je založen na těchto dokumentech, resp. Vnitřních předpisech Správce OÚ:
    a. Organizační řád Správce OÚ,
    b. Spisový řád a skartační plán Správce OÚ, tato směrnice.
4. Systém ochrany osobních údajů definovaný touto směrnicí je navržen a zpracován v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen Nařízení GDPR).
5. Přehled spravovaných agend osobních údajů formou Záznamů o činnostech zpracování je zaměstnancům Správce OÚ k dispozici na ředitelství organizace. Záznamy o činnostech zpracování jsou pravidelně aktualizovány.
6. Směrnice je závazná pro všechny osoby organizačně zařazené do struktury Správce OÚ a pro osoby, které osobní údaje zpracovávají na základě smlouvy uzavřené se Správcem OÚ jakožto správcem osobních údajů; toto ustanovení musí být součástí obsahu uzavřené smlouvy.

III.
Pojmy a definice

1. Pro účely této směrnice a ochrany osobních údajů v rámci Správce OÚ se rozumí:

a. „**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; „**zvláštními kategoriemi osobních údajů**" osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;
b. „**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;
c. „**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;
d. „**omezením zpracování**" označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
e. „**pseudonymizací**" zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;
f. „**anonymizací**" zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů a subjekt údajů není nebo již přestal být identifikovatelným;
g. „**evidencí**" jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;
h. „**správcem**" právnická osoba, orgán veřejné moci nebo agentura, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
i. „**zpracovatelem**" fyzická nebo právnická osoba, orgán veřejné moci nebo agentura, která zpracovává osobní údaje pro správce;
j. „**příjemcem**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty;
k. „**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;
l. „**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;
m. „**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;
n. „**záznamem o činnostech zpracování**" záznamy vedené Správcem OÚ 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;
o. „**dozorovým úřadem**" Úřad pro ochranu osobních údajů;
p. „**Unií**" Evropská unie;
q. **„Členské státy"** Členské státy Evropské unie

r. **„pověřencem ochranou osobních údajů", „pověřencem", „DPO"** pověřenec pro ochranu osobních údajů podle oddílu 4 čl. 37 až 39 Nařízení GDPR.

2. V případě pochybností se shora uvedené pojmy uvedené v tomto článku vykládají dle Nařízení zachování smyslu těchto pojmů v Nařízení uvedeném.

IV.
Rozsah působnosti

1. Vedení Správce OÚ je odpovědné za to, že pravidla ochrany osobních údajů budou zachovávat zaměstnanci, a všechny další osoby, které nakládají s osobními údaji a vystupují v roli uživatelů nebo správců osobních údajů v rámci Správce OÚ.
2. Pravidla ochrany osobních údajů se vztahují rovněž na všechny další subjekty, které pracují s osobními údaji, jichž je Správce OÚ správcem. Tyto subjekty musí být k dodržování zásad ochrany osobních údajů zavázány postupem dle článku XXIV. této směrnice.

V.
Stanovení rolí v systému ochrany osobních údajů

1. Statutární zástupce Správce OÚ
    a. Odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nese Správce OÚ a to zejména, tím, že:
        i. schvaluje Směrnici o nakládání a zpracování s osobními údaji Správce OÚ a její změny a aktualizace,
        ii. vyjadřuje se k osobě, která má vykonávat funkci Pověřence pro ochranu osobních údajů (dále také „Pověřenec" a „DPO"),
        iii. jmenuje Pověřence pro ochranu osobních údajů,
        iv. projednává pravidelnou zprávu o stavu ochrany osobních údajů Správce OÚ,
        v. rozhoduje o přijetí technických, fyzických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR.
2. Pověřenec pro ochranu osobních údajů
    a. Pověřenec je jmenován vedením Správce OÚ a je konkrétní osobou, která plní tyto úkoly při ochraně osobních údajů, za něž zároveň odpovídá:
        i. poskytování informací a poradenství vedoucím pracovníkům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
        ii. monitorování souladu této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů a s vnitřními předpisy Správce OÚ v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti osob, zvyšování povědomí a odborné přípravy zaměstnanců či dalších osob a pracovníků zapojených do operací zpracování a souvisejících auditů;
        iii. spolupráci při vedení centrální evidence zpracování osobních údajů organizačními jednotkami Správce OÚ a její pravidelnou aktualizaci ve spolupráci s organizačními jednotkami;
        iv. spolupráci při vedení centrální evidence udělených souhlasů se zpracováním osobních údajů;
        v. zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji Správce OÚ;
        vi. zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci v rámci Správce OÚ;

vii. poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR v rámci Správce OÚ;
viii. spolupráce s dozorovým úřadem dle Nařízení GDPR;
ix. 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;
x. působení jako kontaktní místo pro subjekty údajů. Subjekty údajů se mohou obracet přímo na Pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Nařízení.

b. 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.
c. Pověřenec pro ochranu osobních údajů je přímo podřízen statutárnímu zástupci Správce OÚ.
d. V souvislosti s plněním svých úkolů nebude Pověřenec propuštěn ani jinak 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.
e. Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí, a to v souladu s právem Unie nebo zákony a právními předpisy České republiky. Pověřenec může plnit i jiné úkoly a povinnosti, které však nesmějí vést ke střetu zájmů jeho činností.

3. Zodpovědné osoby
   a. Ke každé agendě osobních údajů je v rámci Správce OÚ určena Zodpovědná osoba, za řádné a včasné určení zodpovědných osob odpovídá vedení Správce OÚ. Všechny zodpovědné osoby v rámci Správce OÚ jsou uvedeny v Záznamech o činnosti zpracování osobních údajů, které jsou zaměstnancům Správce OÚ k dispozici u DPO a statutárního zástupce. Každá Zodpovědná osoba má právo podat Pověřenci návrh na změnu této směrnice, Záznamu o činnostech zpracování, Posouzení vlivu nebo zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice.
   b. Zodpovědné osoby mají právo a zároveň povinnost:
      i. pro případy vzniku nových druhů osobních údajů tuto skutečnost co nejdříve nahlásit Pověřenci, který spolupracuje při aktualizaci Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
      ii. informovat bezodkladně Pověřence o všech skutečnostech, které mají vliv na aktuálnost Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
      iii. zabezpečit získání souhlasu subjektu údajů, a to v souladu se zákonem, není-li zpracování možné bez tohoto souhlasu;
      iv. zajistit, aby každý zaměstnanec Správce OÚ před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen a proškolen se zásadami ochrany osobních údajů, a s touto směrnicí včetně provedení ověření znalostí a zajistit v roční frekvenci prokazatelné opakování tohoto proškolení;
      v. zajistit, aby každý zaměstnanec Správce OÚ před prvním přístupem ke spravovaným osobním údajům písemně potvrdil, že byl seznámen a proškolen se zásadami ochrany osobních údajů, a s touto směrnicí včetně provedení ověření znalostí;
      vi. 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 a v odůvodněných případech zajistit uzavření smlouvy o zpracování osobních údajů s třetí osobou.

4. Uživatelé osobních údajů

a. Uživatelem osobních údajů, se rozumí zaměstnanec Správce OÚ používající spravované osobní údaje k plnění svých pracovních povinností. Za zaměstnance se považuje též osoba vykonávající činnost dle dohody o pracích konaných mimo pracovní poměr, či v jiném obdobném právním vztahu vůči Správci OÚ.
b. Všichni Uživatelé osobních údajů mají za povinnost:
    i. dodržovat zásady vyplývající z této Směrnice;
    ii. hlásit veškeré bezpečnostní incidenty svému nadřízenému, nebo přímo Pověřenci;
    iii. informovat Pověřence o zjištěných bezpečnostních nedostatcích při ochraně osobních údajů;
    iv. informovat Pověřence o změnách ve způsobu zpracování a nakládání s osobními údaji;
    v. vykonávat další činnosti vyplývající z platných vnitřních předpisů Správce OÚ, především zajistit řádný průběh skartačního řízení v souladu se Spisovým a skartačním řádem Správce OÚ.

5. Správce (Administrátor)
    a. Správce je poskytovatel IT servisu, Správce OÚ, který má na starost provoz a údržbu systémů a aplikací, archivaci a zabezpečení (elektronických) dat uživatelů, a je odpovědný za řízení a implementaci bezpečnosti systémů. Správce (Administrátor) má zpravidla přístup ke všem datům uloženým v informačních systémech Správce OÚ nebo fyzický přístup k zařízením, pomocí nichž jsou tato data zpracovávána.
    b. Správce zabezpečuje spolupráci s jednotlivými uživateli osobních údajů při ochraně osobních údajů uložených ve výpočetní technice, včetně osobních stanic přidělených uživatelům osobních údajů, přenosných počítačů, notebooků, tabletů, mobilních telefonů, smartphonů a jiných obdobných přístrojů.

VI.
Přístup k osobním údajům

1. K osobním údajům mají přístup pouze Zodpovědné osoby, Uživatelé osobních údajů a Správce, jiným osobám se přístup k osobním údajům zapovídá.

VII.
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, přičemž další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se ve smyslu čl. 89 odst. 1 Nařízení GDPR a dle této směrnice nepovažuje za neslučitelné s původními účely („účelové omezení“);
    c. přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);
    d. přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);
    e. uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 Nařízení GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných Nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);

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

2. Zpracovávány mohou být pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Povinnost zpracovávat pouze nezbytné osobní údaje se vztahuje k množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Správní, či jiný spis vedený Uživatelem osobních údajů může obsahovat pouze informace relevantní pro průběh řízení či jinou agendu Uživatele osobních údajů, pro niž je veden. Uživatel osobních údajů odpovídá za minimalizaci údajů, jež jsou zpracovávány dosažení účelu zpracování.
3. Písemnosti obsahující osobní údaje podléhají procesu fyzické a elektronické skartace v souladu se Spisovým a skartačním řádem Správce OÚ, a to včetně písemností a dalších dokumentů „na vědomí", kopií písemností a dalších dokumentů bez čísla jednacího.
4. Pro statistické účely se stanoví povinnost osobní údaje anonymizovat.
5. Tato směrnice stanovuje povinnost všem uživatelům osobních údajů zamezit neoprávněnému přístupu ke shromážděným údajům.

VIII.
Zákonnost zpracování osobních údajů

1. Správce OÚ zpracovává pouze takové osobní údaje, jejichž zpracování je zákonné. Zpracování osobních údajů v odpovídajícím rozsahu je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek:
   a. subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů (dále jen „souhlas"/"souhlas se zpracováním");
   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 Správce OÚ 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 pověřeno Správce OÚ jako správce osobních údajů;
   f. zpracování je nezbytné pro účely oprávněných zájmů Správce OÚ 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 Správcem OÚ jako správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.
2. Účel zpracování osobních údajů musí vycházet z právních základů uvedených v předcházejícím odstavci. 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 pověřen Správce OÚ jako správce osobních údajů.
3. Pokud je zpracování založeno na souhlasu subjektu údajů, je Uživatel osobních údajů povinen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů. Uživatel osobních údajů je dále povinen zajistit a doložit splnění těchto požadavků na souhlas subjektu údajů a na jeho udělení kladených:
   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 Správce OÚ k dispozici u Pověřence.
   b. Subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu, včetně informace o způsobu odvolání uděleného souhlasu. Originál souhlasu uloží Uživatel osobních údajů do spisu.
   c. Pro zpracování zvláštních kategorií osobních údajů (biometrické údaje, fotografie, audio, video, zdravotní stav, sociální postavení a další) se uděluje vždy samostatný souhlas,

oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).

d. Pro zpracování souhlasů s vytvořením kopie občanského průkazu (souhlas podle ustanovení § 15a zákona č. 328/1999 Sb., o občanských průkazech, v platném znění) se uděluje vždy samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).
e. 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 bude subjekt údajů o právu souhlas odvolat prokazatelně poučen. Uživatel osobních údajů zajistí, aby byla splněn právní požadavek spočívající v to, že odvolání souhlasu se zpracováním osobních údajů bude subjektu údajů stejně dostupné jako poskytnutí souhlasu.
f. Uživatel osobních údajů je povinen ve spolupráci se Správcem (Administrátorem) zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat.
g. Uživatel osobních údajů je povinen vést evidenci datových sad, jejichž zpracování je podloženo uděleným souhlasem subjektu údajů.

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

IX.
Opatření pro ochranu osobních údajů

1. Uživatel osobních údajů je povinen dodržovat pravidlo čistého stolu, tzn. neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole či jinde v kanceláři či na pracovišti, po ukončení pracovní doby je každý zaměstnanec povinen takové písemnosti obsahující osobní údaje uložit do uzamykatelných úložných prostor, tyto prostory uzamknout a klíče zajistit tak, aby k nim neměly přístup osoby bez oprávnění přístupu k uloženým osobním údajům. Výjimkou z tohoto pravidla je případ, kdy má zaměstnanec k dispozici samostatnou kancelář, v této kanceláři probíhá úklid výhradně za jeho přítomnosti a klíče od této kanceláře má k dispozici pouze daný zaměstnanec a dále jsou uloženy v prostoru s řízeným přístupem.
2. Uživatel osobních údajů je povinen v případě odchodu z kanceláře, pracovny či jiného pracoviště, kde jsou uloženy osobní údaje, nebo prostředky umožňující přístup k osobním údajům, a kde se již nenachází žádný další zaměstnanec Správce OÚ, zavřít okna a tuto místnost zamknout.
3. Uživatelům osobních údajů se zapovídá ponechat cizí osobu bez dozoru v kanceláři). Uživatel osobních údajů je povinen v případě přítomnosti cizí osoby v kanceláři, v pracovně či na jiném pracovišti, kde jsou uloženy osobní údaje, nebo prostředky umožňující přístup k osobním údajům, a kde se již nenachází žádný další zaměstnanec Správce OÚ, pokud Uživatel osobních údajů hodlá tuto místnost opustit, a v této místnosti se již nenachází žádný další Uživatel osobních údajů či zaměstnanec Správce OÚ, vyprovodit cizí osobu místnosti, tuto místnost uzamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu Uživatele osobních údajů do místnosti.
4. Uživatel osobních údajů je povinen aktivovat spořič obrazovky chráněný heslem, kdykoli se vzdálí od pracovní stanice výpočetní techniky.
5. Uživatel osobních údajů je povinen využívat pro elektronické zpracování osobních údajů výhradně k tomu určené informační systémy Správce OÚ. Užívání pevných disků pro ukládání písemností obsahujících osobní údaje je povoleno pouze v případě, že není možné tuto dokumentaci ukládat do informačních systémů Správce OÚ.
6. Uživatel osobních údajů je povinen udržovat písemnosti obsahující osobní údaje uložené na pevných discích a ve svých e-mailových schránkách v souladu s lhůtami stanovenými pro zpracování dle Spisového a skartačního řádu Správce OÚ a v minimálním rozsahu umožňujícím dosažení účelu zpracování.
7. Uživatel osobních údajů je oprávněn ukládat písemnosti obsahující osobní údaje výhradně na sdílené disky Správce OÚ.

8. Uživatel osobních údajů je povinen využívat pro ukládání listinných dokumentů obsahujících osobní údaje a k ukládání fyzických nosičů, obsahujících osobní údaje v elektronické podobě k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění místnosti uzamknout. Uživatel osobních údajů je povinen k písemnostem obsahujícím osobní údaje přiřazovat řádně a včas skartační znaky dle platného Spisového a skartačního řádu Správce OÚ. To platí i pro písemnosti, obsahující osobní údaje „na vědomí", kopie písemností a další dokumenty bez čísla jednacího či spisové značky.
9. Uživatel osobních údajů je povinen udržovat v tajnosti, tzn. nikomu nesdělovat přístupová oprávnění (přihlašovací jméno a heslo) k informačním systémům Správce OÚ, která mu byla přidělena, tato přístupová oprávnění je zakázáno si zapisovat či jinak poznamenávat (na papír, do souboru, apod.) stejně jako je zakázáno je sdělovat dalším osobám.
10. Uživatel osobních údajů je povinen při tisku písemností obsahujících osobní údaje tyto nikdy neponechávat bez dozoru na tiskárně, a to i tehdy, pokud se tiskárna nachází ve stejné místnosti. To pravidlo obdobně platí též pro použití jiných reprografických či jiných obdobných zařízení.
11. Uživateli osobních údajů se zakazuje přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé e-mailové schránky (např. www.seznam.cz, www.gmail.com apod.).
12. Uživateli osobních údajů se zakazuje zasílat písemnosti obsahující osobní údaje e-mailem bez jejich dodatečného zabezpečení za pomoci šifrování (.ZIP nebo .PDF s heslem). V případě použití šifrování (.ZIP nebo .PDF s heslem) musí být heslo k souboru předáno jiným kanálem (SMS nebo telefonicky).
13. Uživatel osobních údajů se stanovuje je povinen pro předání osobních údajů použít výhradně interní poštu IS, nebo Českou poštu, případně Informační systém datových schránek.
14. Uživateli osobních údajů se zakazuje ukládat na veřejné servery sítě Internet (např. www.uloz.to, www.uschovna.cz apod.) na sociální sítě Facebook, Twitter a další jakékoli písemnosti obsahující osobní údaje bez jejich zabezpečení šifrováním (.ZIP s heslem, .PDF s heslem). Technický přístup na úložiště Internetu, sociální sítě Facebook, Twitter a další je vyhrazen pouze těm předem určeným zaměstnancům, u nichž je takové sdílení dat odůvodněno charakterem jejich pracovní činnosti.
15. Uživateli osobních údajů se zapovídá provádět na svěřené výpočetní technice jakékoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software či připojovat jakákoli Správcem OÚ neschválení technická zařízení, paměťová media, výpočetní techniku, notebooky, mobilní telefony či smartphony nebo tablety.
16. Uživatel osobních údajů je povinen využívat mobilní zařízení Správce OÚ (technická zařízení, paměťová media, výpočetní techniku, notebooky, mobilní telefony či smartphony nebo tablety) pouze při dodržení pravidel pro jejich zabezpečení definovaných Správcem, zejména je povinen použít Správcem nařízené šifrování v případě notebooku a hesla na mobilním telefonu či tabletu.
17. Uživateli osobních údajů se zakazuje využívat k přístupu k informačním systémům a datům Správce OÚ soukromá mobilní zařízení (paměťová media, výpočetní techniku, notebooky, mobilní telefony či smartphony nebo tablety apod.).
18. Uživateli osobních údajů se zakazuje jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.) na svěřených prostředcích (paměťová media, výpočetní technika, notebooky, mobilní telefony či smartphony nebo tablety).
19. Uživatel osobních údajů je povinen v případě tisku na sdílené tiskárně či v případě použití jiného sdíleného obdobného reprografického zařízení tisky obsahující osobní údaje vždy zabezpečit PINem, a to tak, aby byly vytištěny až po zadání PINU na sdílené tiskárně či na jiném sdíleném obdobném reprografickém zařízení uživatelem osobních údajů.
20. Uživateli osobních údajů se zakazuje ukládat na vyměnitelná paměťová média jakékoliv písemnosti obsahující osobní údaje bez jejich zabezpečení pro předávání dat šifrování (.ZIP, .PDF), a stejně tak se mu zakazuje vynášet tato paměťová media mimo prostory Správce OÚ. K ukládání písemností obsahujících osobní údaje jsou uživatelům osobních údajů k dispozici (u Správce IT) HW šifrované flash disky, jež jsou povinni použít. Vyměnitelnými médii se rozumí CD/DVD disky, přepisovatelné CD/DVD, pevné počítačové disky externí, flash disky apod.
21. Každý uživatel osobních údajů či jiný zaměstnanec Správce OÚ, který přichází do styku s písemnostmi obsahujícími osobní údaje uloženými na médiích (CD, DVD, papírové dokumenty, flash paměťové moduly) je povinen zajistit jejich bezpečnou likvidaci (skartování, vymazání, fyzické zničení) v souladu se Spisovým a skartačním řádem Správce OÚ.

22. Klíče od kanceláří, pracoven či jiných pracovišť, kde jsou uloženy či zpracovávány osobní údaje, nebo prostředky umožňující přístup k osobním údajům Správce OÚ vydává uživateli osobních údajů pouze prokazatelným způsobem, když o jejich vydání a vrácení bude vedena příslušná evidence. Správce OÚ podrobí evidenci a kontrole ukládání a zabezpečení náhradních klíčů od kanceláří, pracoven či jiných pracovišť, kde jsou uloženy či zpracovávány osobní údaje, nebo prostředky umožňující přístup k osobním údajům.
23. Uživatelé osobních údajů nejsou oprávněni hovořit (osobně ani telefonicky) o osobních údajích v přítomnosti třetích osob. Tato povinnost se vztahuje též na předávání informací zaměstnancům Správce OÚ, kteří nemají k těmto osobním údajům přístup.

X.
Předávání osobních údajů

1. Dokumenty obsahující osobní údaje, jakožto i osobní údaje samotné je v elektronické podobě povoleno předávat příjemcům mimo Správce OÚ pouze prostřednictvím systému datových schránek. V případech, kdy není možné dokumenty obsahující osobní údaje, jakožto i osobní údaje samotné předat prostřednictvím systému datových schránek nebo ve fyzické podobě, bude předání realizováno za využití šifrování (například PDF nebo .ZIP), když heslo k souboru bude předáno jiným kanálem (SMS nebo telefonicky).

XI.
Zveřejňování osobních údajů

1. Při zveřejňování osobních údajů budou provedena opatření, která zajistí, že veškeré zveřejňované osobní údaje (text, audio, video) budou anonymizovány v rozsahu zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění uloženého legislativou. To znamená, že zveřejněné osobní údaje budou anonymizovány ve všech případech, kdy zákon nestanoví jinak. Výjimkou z tohoto pravidla jsou pouze ty případy zveřejnění osobních údajů, kdy ke zveřejnění byl subjektem údajů udělen souhlas dle Čl. VII. odst. 1 této směrnice.
2. Opatření zajišťující anonymizaci osobních údajů budou provedena u osobních údajů třetích osob ve smlouvách, které jsou zveřejněny v Registru smluv.
3. Při pořizování jakýchkoliv záznamů z akcí pořádaných Správcem OÚ budou účastníci akce informováni o pořizování audio/video dokumentace a o účelu o účelu pořizování audio/video dokumentace. Bude-li pořízení audio/video dokumentace zpracováním osobních údajů, je Uživatel osobních údajů povinen zajistit řádné a včasné udělení souhlasu subjektu údajů se zpracováním jeho osobních údajů.
4. V případě pořizování fotografické nebo video dokumentace z veřejných akcí Správce OÚ, bude zajištěno informování účastníků o pořizování této dokumentace za účelem zveřejnění na webových stránkách Správce OÚ apod. Pracovníci pořizující tuto dokumentaci musí být viditelně a výrazně označeni. Ustanovení předcházejícího odstavce této směrnice tu platí obdobně.
5. Fotografie zaměstnanců Správce OÚ budou pořizovány a zveřejňovány na webových stránkách Správce OÚ anebo jinými způsoby, pouze tehdy, pokud k jejich pořízení a zveřejnění byl zaměstnancem jakožto subjektem údajů udělen souhlas dle Čl. VII. Odst. 1 této směrnice. Zveřejnění fotografií zaměstnanců Správce OÚ bez takového souhlasu je možné pouze u osob, u kterých je to odůvodnitelné s ohledem na výkon jejich činnosti či postavení v řídící struktuře Správce OÚ.

XII.
Získávání informací od subjektu údajů

1. Odpovědný zaměstnanec Správce OÚ či Uživatel osobních údajů v případě získání osobních údajů poskytne subjektu údajů předem tyto informace:
    a. totožnost a kontaktní údaje Správce OÚ a jeho odpovědného zaměstnance (Uživatele osobních údajů);
    b. kontaktní údaje Pověřence;
    c. účely zpracování, pro které jsou získávané osobní údaje určeny, a právní základ pro jejich zpracování;

d. oprávněné zájmy Správce OÚ nebo třetí strany v případě, že je zpracování založeno na opodstatněném zájmu Správce OÚ 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 Správce OÚ jako od 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. o právu podat stížnost u dozorového úřadu;
j. o skutečnosti, 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. Splnění informační povinnosti podle bodu předcházejícího odstavce může být zajištěno zveřejněním Informačního memoranda na webových stránkách Správce OÚ.
3. Pokud Správce OÚ 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.

XIII.
Práva subjektu údajů

1. Subjekt je oprávněn může uplatnit u Správce OÚ, jako správce osobních údajů tato právo na:
   a. přístup k osobním údajům
   b. opravu a výmaz osobních údajů
   c. omezení zpracování osobních údajů
   d. přenositelnost osobních údajů
   e. vznesení námitky
2. Naplnění práv subjektů údajů zajišťuje Pověřenec je povinen zajistit splnění práv subjektu údajů, jež byla u Správce OÚ uplatněna v souladu s Nařízením GDPR.
3. Pokud je pro zajištění práv subjektů údajů nutné zapojení více útvarů Správce OÚ, zajišťuje jejich koordinaci a shromáždění potřebných informací Pověřenec.
4. Způsob podání žádosti o naplnění práv subjektů údajů je zveřejněn na webových stránkách Správce OÚ, případně dalšími vhodnými způsoby.
5. Subjektu údajů budou poskytovány informace v souladu se zásadami zpracování osobních údajů dle čl. 7 této směrnice a to stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené dítěti, či osobě, u níž byla svéprávnost omezena, či u níž tento přístup odůvodňuje zvláštní důvody.
6. Informace jsou subjektu údajů poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (předložení dokladu totožnosti, či použití datové schránky).
7. Informace jsou subjektu údajů poskytovány písemně nebo jinou formou, připuštěna je ve vhodných případech i elektronická forma. Pokud si to subjekt údajů vyžádá, budou informace poskytnuty pouze ústně.
8. Informace budou subjektu údajů poskytnuty bez zbytečného odkladu a nejpozději ve lhůtě do jednoho kalendářního měsíce od doručení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další maximálně dva kalendářní měsíce, kdy subjekt údajů musí být o takovém odůvodněném prodloužení lhůty k poskytnutí údajů vyrozuměn nejpozději ve lhůtě do jednoho kalendářního měsíce od doručení žádosti.
9. Pokud opatření, o něž subjekt údajů požádal, nejsou provedena, bude subjekt údajů bezodkladně a nejpozději ve lhůtě do jednoho kalendářního měsíce od doručení žádosti informován o důvodech

nerealizování opatření a o jeho možnosti podat stížnost u dozorového úřadu a o možnosti žádat o soudní ochranu dle Nařízení o GDPR.

10. Zjevnou nedůvodnost nebo nepřiměřenost žádosti je uživatel osobních údajů, či jiný zaměstnanec Správce OÚ, který žádost subjektu údajů v rámci své činnosti u Správce OÚ vyřizuje, povinen odůvodnit a zdokumentovat.

XIV.
Právo subjektu údajů na přístup k osobním údajům

1. Subjekt údajů má právo získat od Správce OÚ jako správce osobních údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud jsou zpracovávány, 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 Správce OÚ jako od 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. Správce OÚ jako správce osobních údajů poskytne subjektu údajů kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může Správce OÚ 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).

XV.
Oprava a výmaz osobních údajů

1. Subjekt údajů má právo na to, aby Správce OÚ jako správce osobních údajů bez zbytečného odkladu opravil 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 Správce OÚ jako správce osobních údajů bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a Správce OÚ 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 Správce OÚ jako správce osobních údajů vztahují.
3. Jestliže Správce OÚ jako správce osobních údajů osobní údaje zveřejnil je povinen je podle odstavce 2 této směrnice vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně všech technických opatření k tomu, aby informoval zpracovatele, kteří tyto osobní údaje

zpracovávají, že je subjekt údajů žádá, aby též provedli výmaz veškerých odkazů 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 Správce OÚ jako na správce osobních údajů vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce OÚ pověřeno;
    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.
5. Požadavek subjektu údajů na výmaz nelze splnit, pokud je zpracování nezbytné pro splnění právní povinnosti.

XVI.
Právo na omezení zpracování

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

XVII.
Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

1. Správce OÚ 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. Správce OÚ jako správce osobních údajů informuje subjekt údajů o těchto příjemcích, pokud tuto informaci subjekt údajů požaduje.
2. Splnění informační povinnosti podle předchozího odstavce může být zajištěno zveřejněním Informačního memoranda na webových stránkách Správce OÚ.

XVIII.
Právo na přenositelnost údajů

1. Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl Správci OÚ jako správci osobních údajů, ve strukturovaném, běžně používaném a strojově čitelném formátu, a má právo předat tyto údaje jinému správci, a to v případě, že:
    a. zpracování je založeno na uděleném souhlasu se zpracováním osobních údajů nebo na uzavřené smlouvě, a současně
    b. zpracování se provádí v elektronické podobě.
2. Subjekt údajů má právo na to, aby Správce OÚ jako správce osobních údajů osobní údaje předal přímo druhému správci, je-li to technicky proveditelné.
3. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce OÚ jako správce osobních údajů pověřeno.
4. Uplatněním práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

XIX.
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. Správce OÚ jako správce osobních údajů osobní údaje v takovém případě dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo je zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků.
2. Správce OÚ subjekt údajů o právu vznést námitku výslovně zřetelně a odděleně od jakýchkoli jiných informací poučí, a to nejpozději v okamžiku první komunikace se subjektem údajů.

XX.
Řešení případů porušení zabezpečení osobních údajů

1. Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec Správce OÚ neprodleně svému přímému nadřízenému (vedoucímu zaměstnanci) a Pověřenci pro ochranu osobních údajů.
2. Hlášení bude obsahovat alespoň tyto informace:
    a. popis povahy daného případu porušení zabezpečení osobních údajů, pokud je to možné, s uvedením kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených osobních údajů;
    b. popis pravděpodobných důsledků porušení zabezpečení osobních údajů pro Správce OÚ jako správce osobních údajů a pro subjekty údajů a jich práva;
    c. návrh okamžitých opatření k zamezení dalšímu porušení zabezpečení osobních údajů a návrh bezprostředních nápravných opatření.
3. Pověřenec pro ochranu osobních údajů ve spolupráci se Zodpovědnou osobou, Uživateli osobních údajů, Správcem, relevantními zpracovateli osobních údajů, případně dalšími relevantními zaměstnanci Správce OÚ, neprodleně rozhodne o dalším postupu.
4. Pověřenec pro ochranu osobních údajů neprodleně informuje starostu či statutárního zástupce Správce OÚ 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 vedoucímu pracovníku (starostovi či statutárnímu zástupci) Správce OÚ ke schválení návrh nápravných opatření pro zamezení opakování obdobného porušení zabezpečení osobních údajů. Nápravné opatření bude obsahovat kroky obnovy a postup k zamezení porušení zabezpečení a jeho opakování, termíny realizace opatření, jména zaměstnanců odpovědných za jejich splnění. Návrh nápravných opatření musí být konzultován s relevantními Zodpovědnými osobami, které ho svým podpisem potvrdí. Realizace nápravných opatření podléhá schválení starosty či statutárního zástupce Správce OÚ.
6. Pověřenec pro ochranu osobních údajů provádí kontrolu plnění nápravných opatření a výsledky předkládá starostovi či statutárnímu zástupci Správce OÚ v termínech k tomu určených nápravným opatřením.

XXI.
Činnost při zjištění porušení zabezpečení osobních údajů

1. Jakékoli porušení zabezpečení osobních údajů nebo ztrátu dostupnosti osobních údajů (dále jen „incident"), nebo podezření takového porušení, je zaměstnanec Správce OÚ povinen hlásit Pověřenci pro ochranu osobních údajů a svému nadřízenému.
2. Podezření na incident se posuzuje pro potřeby postupu podle této směrnice stejně jako incident, dokud není zjištěno, že incident nevznikl.
3. V případě incidentu, spočívajícího ve ztrátě dostupnosti osobních údajů se ustanovení článku XXI. použijí přiměřeně.
4. Pověřenec pro ochranu osobních údajů je odpovědný za řízení reakce na incident.
5. Pověřenec pro ochranu osobních údajů spolupracuje při řízení reakce na incident s vedoucími zaměstnanci Správce OÚ a pokud je to potřebné nebo nutné, se smluvními partnery Správce OÚ a s dalšími orgány veřejné správy. Spolupráce Pověřenec s třetími osobami je podmíněna schválením starosty či statutárním zástupcem Správce OÚ.
6. Pověřenec pro ochranu osobních údajů vede dokumentaci činností a komunikace při reakci na incident tak, aby byla úplná a průkazná.
7. Úkony v reakci na incident se provádějí bez zbytečného odkladu, a pokud je to možné, okamžitě. Pokud některý z potřebných úkonů vyžaduje omezení dostupnosti informací nebo služby, informuje o tom Pověřence, starostu či statutárního zástupce Správce OÚ.
8. Hlavními cíli 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 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 Úřadu, tak, aby se předešlo incidentům u dalších správců.
9. Činnost podle tohoto článku bude ukončena, jestliže o tom rozhodne Pověřenec na základě předložené zprávy a zabezpečených podkladů a informací, nebo pokud se prokáže, že k incidentu nedošlo.

XXII.
Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Jakékoli porušení zabezpečení osobních údajů Správce OÚ jako správce osobních údajů prostřednictvím Pověřence bez zbytečného odkladu nejpozději 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. Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu Správci OÚ jako správci osobních údajů.
3. 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 nebo jiného kontaktního místa, které může poskytnout bližší informace;
c. popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
d. popis opatření, která Správce OÚ jako správce přijalo nebo navrhlo k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

4. Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Pověřenec 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 ustanovením směrnice.

XXIII.
Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

1. Pokud je pravděpodobné, že případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Správce OÚ jako správce osobních údajů prostřednictvím Pověřence toto porušení bez zbytečného odkladu subjektu údajů.
2. V oznámení 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. XXII. této Směrnice.
3. Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
   a. Správce OÚ jako správce osobních údajů zavedlo náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, a to zejména taková opatření, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (kupř. šifrování);
   b. Správce OÚ jako správce osobních údajů přijalo následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již s vysokou pravděpodobností neprojeví;
   c. Oznámení by vyžadovalo nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo jiného podobného opatření.
4. Jestliže Správce OÚ jako správce osobních údajů dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámilo, je dozorový úřad oprávněn, požadovat, aby oznámení bylo provedeno.

XXIV.
Zpracovatel

1. Pokud má být zpracování provedeno pro Správce OÚ jako pro správce osobních údajů, využije Správce OÚ pouze ty zpracovatele, kteří poskytují dostatečné záruky, že zavedou dostatečná technická a organizační opatření, jež zajistí, že zpracování bude splňovat požadavky Nařízení GDPR a této směrnice a že byla zajištěna ochrana práv subjektu údajů.
2. Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího písemného povolení Správce OÚ jako správce osobních údajů k čemuž bude Správcem OÚ zavázán. Zpracovatel informuje předem Správce OÚ jako správce osobních údajů o zapojení dalších zpracovatelů nebo o nahrazení a změnách zpracovatelů, a poskytne tak Správci OÚ jako správci osobních údajů příležitost vyslovit vůči těmto změnám námitky.
3. Správce OÚ uzavře se zpracovatelem písemnou smlouvu, která stanoví práva a povinnosti zpracovatele při zpracování. Zodpovědná osoba je povinna zajistit, aby s každým zpracovatelem byla před zahájením zpracování uzavřena Smlouva o zpracování osobních údajů, která zavazuje zpracovatele vůči Správci OÚ jako správci osobních údajů a v níž je stanoven předmět a doba trvání

zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Vzor Smlouvy o zpracování osobních údajů je umístěn u DPO.

XXV.
Kontrola dodržování ustanovení směrnice

1. Vedoucí zaměstnanci Správce OÚ zajistí kontrolu plnění povinností vyplývajících z ustanovení této Směrnice pro nakládání s osobními údaji v mezích své působnosti.
2. Vedoucí pracovníci Správce OÚ zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všichni zaměstnanci Správce OÚ včetně proškolení a ověření znalostí směrnice a povinností na úseku ochrany osobních údajů.
3. Pověřenec odpovídá za pravidelné testování, posuzování a hodnocení účinnosti zavedených organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji Správce OÚ. Při provádění kontrolních činností jsou všichni zaměstnanci Správce OÚ povinni poskytovat Pověřenci součinnost. O provedených zjištěních vede Pověřenec pro ochranu osobních údajů prokazatelnou dokumentaci, kterou předkládá na vědomí statutárnímu zástupci Správce OÚ.
4. Pověřenec předkládá doporučení ke změnám organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování osobních údajů statutárnímu zástupci Správce OÚ ke schválení vždy, když je takových změn zapotřebí.

XXVI.
Revize směrnice

1. Správce OÚ provede revizi této Směrnice pro nakládání s osobními údaji v případě potřeby, nejméně však jednou za dva roky a vždy, když revizi navrhne Pověřenec.
2. Za zpracování, prosazení, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá pověřený zaměstnanec Správce OÚ.
3. Tato směrnice nabývá platnosti a účinnosti dne 1.8. 2020 a nahrazuje Vnitřní předpis o ochraně osobních údajů ze dne 22.2.2017, který se tímto ruší.

Revize první s platností od 1.4.2024
(nový statutární zástupce, nové logo organizace, korektury)

V Příbrami dne 1. 4. 2024

Schválil:

Mgr. Barbora Vacková, ředitelka CSZS

CENTRUM SOCIÁLNÍCH A ZDRAVOTNÍCH SLUŽEB MĚSTA PŘÍBRAM

8

Centrum sociálních a zdravotních služeb města Příbram
Brodská 100, 261 01 Příbram VIII • IČ: 47067071
T: 318 629 057 • E: info@centrumpribram.cz
www.centrumpribram.cz