****

Sp.zn. OT/xx/2023

Č.j. MUHU/xxx/2023/Sa

Směrnice o nakládání s osobními údaji

směrnice č. SM/5/2023/RM

|  |  |  |  |
| --- | --- | --- | --- |
| Organizace:  (dále „Organizace“) | Město Humpolec, Horní náměstí 300, 396 22 Humpolec  IČ 00248266 | | |
| Vypracoval: | Ing. Milan Seidler  Mgr. Jiří Fiala, tajemník MěÚ | | |
| Schválil: | Rada města Humpolce, usnesením č. xxx/15/RM/2023 | Dne 26/7 2023 |
| Kontrolou provádění směrnice je pověřen: | Mgr. Jiří Fiala, tajemník MěÚ | | |
| Datum platnosti od: | 27/7 2023 | | |
| Datum účinnosti od: | 1/8 2023 | | |
| Tato směrnice ruší interní směrnici č. 1/2015, upravující nakládání s osobními údaji u Městského úřadu Humpolec ze dne 1. února 2015.  Tato směrnice na základě § 110 odst. 4 písm. e) zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů, upravuje nakládání s osobními údaji 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 „GDPR“) a zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „zákon o zpracování osobních údajů“). | | | |

Část I.

Základní ustanovení a pojmy

1. Účelem interního předpisu je:
2. informovat zaměstnance organizace o základních pojmech a procesech souvisejících se zpracováním osobních údajů, vysvětlit dané pojmy a procesy, a to mimo jiné uvedením pro organizaci typických konkrétních případů nebo činností,
3. vymezit práva a povinnosti zaměstnanců organizace související se zpracováním osobních údajů.
4. Interní předpis upravuje
5. základní rámec činností a postupů při zpracování osobních údajů v organizaci,
6. základní procesy zabezpečení osobních údajů v organizaci,
7. činnosti a postupy zaměstnanců organizace, případně dalších osob při zpracování osobních údajů v organizaci.
8. Interní předpis se vztahuje na
9. zaměstnance organizace,
10. osoby, které v souvislosti s plněním smluvních závazků zpracovávají osobní údaje a které se zavázaly k postupu v souladu s tímto interním předpisem.
11. Vysvětlení základních pojmů
12. Osobní údaj je jakákoli informace o identifikované nebo identifikovatelné fyzické osobě. Fyzická osoba se považuje za identifikovanou nebo identifikovatelnou, jestliže ji lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor nebo kombinaci identifikátorů, například jméno, datum narození, adresa trvalého pobytu, apod.
13. Zvláštní kategorii osobních údajů (také označeno jako citlivé osobní údaje) pro účely této směrnice jsou údaje spadající do zvláštní kategorie osobních údajů ve smyslu čl. 9 nařízení GDPR. Tvoří je:
    * osobní údaje vypovídající o rasovém nebo etnickém původu, např. údaj o národnosti fyzické osoby,
    * osobní údaje vypovídající o politických názorech, náboženském vyznání, filozofickém přesvědčení nebo členství v odborech,
    * genetické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, např. sliny v případě testování na přítomnost návykové látky,
    * biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, např. otisky prstů, …
    * údaje o zdravotním stavu, např. informace o nemoci, postižení, riziku onemocnění, poskytovaném podpůrném opatření, o úrazu; naopak není údajem o zdravotním stavu údaj o tom, že zaměstnanec je zdravotně způsobilý vykonávat práci nebo uchazeč o vzdělání je zdravotně způsobilý se vzdělávat v daném oboru vzdělání,
    * údaje o sexuálním životě, sexuální orientaci,
    * osobní údaje týkající se rozsudků v trestních věcech a trestných činů fyzické osoby či souvisejících bezpečnostních opatření ve smyslu čl. 10 nařízení GDPR.
14. Osobní údaje dětí - k těmto osobním údajům je nutno přistupovat zvlášť citlivým způsobem a zabezpečit je jako citlivé osobní údaje.
15. Subjekt údajů je osoba, které se zpracovávané osobní údaje týkají. V rámci organizace to jsou zaměstnanci vlastní organizace, tak i třetí osoby – občané, zaměstnanci jiných orgánů státní správy a územní samosprávy, zaměstnanci dodavatelských/odběratelských firem, apod.
16. Správcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Pro účely tohoto interního předpisu je správcem Organizace.
17. Zpracovatel je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. V případě Organizace je zpracovatelem např. externí společnost, která vede mzdové účetnictví, poskytovatel cloudového řešení sloužícího ke zpracování osobních údajů; smluvní lékař.
18. Příjemcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty. Za příjemce se dle nařízení GDPR nepovažuje orgán veřejné moci, který získává osobní údaje v rámci zvláštního šetření. Zvláštním šetřením se chápe činnost, která neprobíhá plánovaně a která je vyvolána určitou nestandardní situací (např. šetření trestného činu Policií ČR, apod.). Orgánu veřejné moci je sice v tomto případě osobní údaj obdrží, avšak pro účely GDPR se za příjemce nepovažuje.
19. Právní důvody zpracování jsou důvody, na základě kterých, dochází k legálnímu zpracování osobních údajů. Jedná se o následující právní důvody:
    * plnění právní povinnosti správce,
    * plnění povinnosti vyplývající ze smlouvy,
    * ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
    * plnění úkolů ve veřejném zájmu, nebo při výkonu veřejné moci,
    * oprávněný zájem správce, kdy zpracování je nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce, nebo jiné dotčené osoby. Takové zpracování osobních údajů však nemůže být v rozporu s právem subjektu údajů na ochranu jeho soukromí a osobního života,
    * udělení souhlasu subjektem údajů.

Základní činnosti organizace a právní důvody zpracování osobních údajů jsou uvedeny v materiálech, kterými organizace plní informační povinnost správce dle čl. 13 GDPR nebo dle čl. 14 GDPR a dalšími prostředky. Těmito jsou zejména:

* + základní informace o zpracování osobních údajů a právech subjektů údajů organizací zveřejněné na internetových stránkách organizace,
  + seznam činností, v rámci kterých jsou zpracovávány osobní údaje,
  + plnění informační povinnosti v rámci formulářů úřadu a dokumentů úřadu souvisejících s daným zpracováním osobních údajů,
  + ústní poučení občana o zpracování osobních údajů v rámci projednávané činnosti referentem úřadu.

1. Zpracováním osobních údajů je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je:
   * shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění,
   * vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění,
   * seřazení či zkombinování, omezení, výmaz nebo zničení.
   * Zpracováním je i evidence osobních údajů – evidencí se rozumí jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný nebo rozdělený podle funkčního nebo zeměpisného hlediska (např. seznam plátců, apod.)
2. Službou informační společnosti se rozumí každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb ve smyslu čl. 1 odst. 1 písm. b) Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. 9. 2015, o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti. Za službu informační společnosti se považuje například vedení portálu občana nebo jiného obdobného portálu správcem nebo poskytování veřejného Wi-Fi připojení správcem, je-li taková služby zřízena. Dle § 7 zákona o zpracování osobních údajů souhlas se zpracováním osobních údajů při čerpání služeb informační společnosti může dát občan od dosažení 15 let svého věku.
3. Organizací se rozumí Městský úřad Humpolec, Horní náměstí 300, 396 22 Humpolec, IČ: 00248266.
4. Útvarem se rozumí odbor, oddělení příp. jiný organizační prvek dle Organizačního řádu organizace.
5. Pracovníkem se rozumí zaměstnanec nebo jiná osoba zajišťující uvedenou službu pro organizaci.
6. Osobou oprávněnou ke zpracování osobních údajů je:
   * pověřený zaměstnanec organizace,
   * veřejný funkcionář organizace dle zákona č. 159/2006 Sb. o střetu zájmů, ve znění pozdějších předpisů, u kterého vyplývá nutnost zpracování osobních údajů z jeho pracovního nebo funkčního zařazení a předmětu činnosti,
   * člen komise rady či výboru zastupitelstva obce, jestliže zpracovávají osobní údaje v rámci plnění povinností člena komise či výboru,
   * člen rady a zastupitelstva.

Část II.

Základní etapy procesu zpracování osobních údajů

1. Osobní údaje jsou získány od subjektu údajů
2. Organizace získává osobní údaje zpravidla přímo od subjektu údajů. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů informace dle čl. 13 GDPR. Jako okamžik získání osobních údajů se chápe okamžik, ve kterém subjekt údajů např. vyplňuje formulář dokumentu na základě kterého jsou osobní údaje evidovány v rámci dané evidence; vyplňuje formulář souhlasu se zpracováním osobních údajů apod. Proto jsou údaje dle čl. 13 GDPR subjektů údajů sděleny
   * písemně (v jednotlivých formulářích na část, ve které je subjekt údajů informován dle čl. 13 GDPR, navazuje část, ve které subjekt údajů vyplňuje jednotlivé údaje), a/nebo
   * elektronicky (informace dle čl. 13 GDPR jsou subjektu údajů stále uveřejněny na internetových stránkách organizace).

Organizace nemusí subjekt údajů informovat o skutečnostech, pokud subjekt údajů informace o těchto skutečnostech již má, nebo je má v určité míře. Organizace však upřednostňuje postup, při kterém jsou subjektu údajů informace sdělovány přehledně a uceleně, a to vždy v souvislosti s určitou skupinou případů zpracování osobních údajů. Z tohoto důvodu jsou informace dle čl. 13 GDPR subjektu údajů zpracovávány a sdělovány subjektu údajů v celém rozsahu dle čl. 13 GDPR.

1. Poté, co organizace informovala subjekt údajů dle čl. 13 GDPR, správce začíná osobní údaje zpracovávat, neboť je shromažďuje.
2. Dále správce provádí jednotlivé činnosti zpracování, např. osobní údaje zaznamenává, ukládá, zpřístupňuje.
3. Proces zpracování osobních údajů se uzavírá likvidací osobních údajů, tj. fyzickým zničením nosiče osobních údajů, fyzickým vymazáním nebo jejich trvalým vyloučením ze zpracování a výmazem elektronického záznamu osobních údajů. Plánovaná lhůta pro výmaz je uvedena v záznamu o činnosti zpracování. Lhůtou pro výmaz je údaj o skartačních lhůtách nosičů osobních údajů, které organizace stanoví jako veřejnoprávní původce archiválií podle zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, na základě právních předpisů, nebo podle svého uvážení (jestliže lhůta není stanovena právním předpisem).
4. Výmaz údajů nelze provést v případě, kdy zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, výslovně ukládá, že jde o archiválii.
5. Osobní údaje nejsou získány od subjektu údajů
6. Některé osobní údaje organizace získává od osoby odlišné od subjektu údajů. Jedná se např. o osobní údaje rodinných příslušníků u zaměstnanců.
7. V souladu se zákonem Správce získává příp. ověřuje osobní údaje prostřednictvím celostátně provozovaných informačních systémů, zejména informačního systému základních registrů.
8. Správce začíná osobní údaje zpracovávat, neboť je shromažďuje.
9. Dále správce provádí jednotlivé činnosti zpracování.
10. Proces zpracování osobních údajů se uzavírá likvidací osobních údajů, tj. fyzické zničení nosiče osobních údajů, fyzické vymazání nebo jejich trvalé vyloučení ze zpracování a výmaz elektronického záznamu osobních údajů. Plánovaná lhůta pro výmaz je uvedena v záznamu o činnosti zpracování. Lhůtou pro výmaz je údaj o skartačních lhůtách nosičů osobních údajů, které organizace stanoví jako veřejnoprávní původce archiválií podle zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, na základě právních předpisů, nebo podle svého uvážení (jestliže lhůta není stanovena právním předpisem).
11. Jestliže osobní údaje nebyly získány od subjektu údajů, poskytne správce subjektu údajů informace dle čl. 14 GDPR.
12. Správce poskytne informace dle čl. 14 GDPR
    * v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
    * nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo
    * nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.
13. Proto jsou údaje dle čl. 14 GDPR subjektů údajů sděleny
    * písemně, a/nebo
    * elektronicky (informace dle čl. 14 GDPR jsou uveřejněny na internetových stránkách organizace).
14. Správce subjektu údajů informace dle čl. 14 GDPR neposkytne, jestliže
    * subjekt údajů již uvedené informace má,
    * ukáže se, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí,
    * získávání nebo zpřístupnění osobních údajů je výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů.
15. V případě, kdy organizace poskytuje informace dle čl. 14 GDPR, upřednostňuje postup, při kterém jsou subjektu údajů informace sdělovány přehledně a uceleně, a to vždy v souvislosti s určitou skupinou případů zpracování osobních údajů. Z tohoto důvodu jsou informace dle čl. 14 GDPR subjektu údajů zpracovávány a sdělovány subjektu údajů kompletně, v celém rozsahu dle čl. 14 GDPR.

Část III. Zásady zpracování osobních údajů a s nimi spojené povinnosti zaměstnanců

| **Zásady zpracování o.ú.** | **Pravidla stanovená správcem** | **Povinnosti zaměstnance** |
| --- | --- | --- |
| Zásada zákonnosti, korektnosti a transparentnosti | Správce aplikuje právní důvody zpracování osobních údajů na podmínky organizace.  Správce stanoví pravidla uživatelsky přívětivého, stručného a srozumitelného informování subjektů údajů. | Určení vedoucí zaměstnanci seznámí zaměstnance s tím, jak se používají právní důvody zpracování v konkrétních podmínkách a při konkrétních činnostech.  Zaměstnanci zpracovávají osobní údaje pouze na základě právních důvodů.  Určený vedoucí zaměstnanec průběžně kontroluje, zda jsou osobní údaje zpracovávány pouze na základě právních důvodů a zda jsou subjekty údajů stručně a srozumitelně informovány o pravidlech zpracování osobních údajů. |
| Účelové omezení | Správce stanoví účel zpracování osobních údajů. | Zaměstnanec zpracovává osobní údaje pouze za tím účelem, za kterým byly shromážděny.  Určený vedoucí zaměstnanec pravidelně kontroluje dodržování zásahy účelového omezení zpracování osobních údajů. |
| Minimalizace údajů | Správce zpracovává osobní údaje pouze v takovém rozsahu, který je nezbytný k dosažení určitého účelu. | Zaměstnanci zpracovávají osobní údaje pouze v tom rozsahu, který stanoví zaměstnavatel.  Určený vedoucí zaměstnanec pravidelně provádí kontrolu rozsahu zpracovávaných osobních údajů. |
| Přesnost | Správce zpracovává přesné a aktualizované osobní údaje. | Určení zaměstnanci (vedoucí zaměstnanec, personalista, referent) pravidelně provádí kontrolu přesnosti zpracovávaných osobních údajů a zajišťují jejich opravu a aktualizaci. |
| Omezení uložení | Osobní údaje jsou uloženy pouze po nezbytnou dobu, tuto dobu stanoví správce. | Určení zaměstnanci sledují dobu, po kterou je osobní údaj ukládán u správce. Po uplynutí této doby zajišťují archivaci dokumentů nebo jejich skartaci. |
| Integrita a důvěrnost | Správce přijímá vhodná personální, organizační a technická opatření k zabezpečení osobních údajů uvedená zejména v Bezpečnostní směrnici. | Zaměstnanci jsou povinni respektovat správcem stanovená pravidla k zabezpečení osobních údajů. |

Část IV. Povinnosti v souvislosti se zpracováním osobních údajů

1. Každá oprávněná osoba je povinna:
2. zachovávat mlčenlivost o zpracovávaných osobních údajích. Povinnost mlčenlivosti trvá i po skončení pracovněprávního poměru či funkčního nebo smluvního vztahu k Organizaci,
3. zpracovávat osobní údaje pouze na základě právních důvodů; v případě pochybnosti o právním základu zpracování je povinna konzultovat zpracování osobních údajů s vedoucím jeho útvaru, případně s pověřencem pro ochranu osobních údajů,
4. zpracovávat osobní údaje pouze za tím účelem, za kterým byly shromážděny a v rozsahu, který je stanoven pro každou jednotlivou činnost; v případě pochybnosti je povinna konzultovat zpracování osobních údajů s vedoucím jeho útvaru, případně s pověřencem pro ochranu osobních údajů,
5. počínat si tak, aby neohrozila ochranu osobních údajů zpracovávaných Správcem; zamezit nahodilému a neoprávněnému přístupu třetích osob k osobním údajům, které organizace zpracovává, pokud zjistí porušení ochrany osobních údajů, neoprávněné použití osobních údajů, zneužití osobních údajů nebo jiné neoprávněné jednání související s ochranou osobních údajů, a je povinna bezodkladně zabránit dalšímu neoprávněnému nakládání s osobními údaji, zejména zajistit znepřístupnění, a ohlásit tuto skutečnost vedoucímu jeho útvaru nebo tajemníkovi úřadu,
6. neshromažďovat osobní údaje bez jednoznačného pokynu vedoucího zaměstnance nebo bez ověření, že je takový postup možný,
7. nezveřejňovat, nezpřístupňovat osobní údaje bez právního důvodu; nezpřístupnit osobní údaje osobám, které neprokáží právo s nimi nakládat (cizí osoby, instituce),
8. neposkytovat bez právního důvodu žádnou formou osobní údaje zaměstnanců a občanů cizím osobám a institucím, tedy ani telefonicky ani mailem ani při osobním jednání,
9. zpracovávat hodnocení, posudky obsahující osobní údaje určené pro jiné subjekty (např. pro potřeby soudního řízení) pouze na základě právního důvodu,
10. na pracovišti dodržovat pravidla bezpečnosti práce včetně požárních a poplachových pravidel tak, aby nedošlo ke zničení uložených písemností a digitálních záznamových médií s osobními údaji v důsledku požáru, potopy nebo jiné havárie,
11. informace obsahující osobní údaje získané z Informačních systémů zpřístupňovat a předávat jen jiným oprávněným osobám v rozsahu nezbytném pro výkon jejich agendy. V případě, že je přeprava nosičů s osobními údaji určenými jiným oprávněným osobám svěřena jiným subjektům, je poskytující oprávněná osoba povinna tyto nosiče umístit samostatně podle jednotlivých adresátů v uzavřených obalech (např. zalepená obálka nebo krabice s přelepem a podpisem či razítkem). O odeslaných nebo předaných osobních údajích musí být veden záznam (za záznam je možno považovat odeslanou datovou zprávu, poštovní doručenku, odeslanou zprávu ve spisové službě),
12. kopie nosičů s osobními údaji či osobních údajů samých pořizovat jen v případech nezbytných pro výkon pracovní činnosti (nelze-li účelu dosáhnout jinak), na kopie nosičů se aplikují stejná bezpečnostní opatření a záruky jako na originál,
13. neukládat dokumenty obsahující osobní údaje na externí hardware (USB, CD, DVD apod.) nebo software, ledaže to oprávněné osobě povolí vedoucí útvaru, a to jednotlivě, nebo pro typově stejné případy. Oprávněná osoba je vždy povinna ukládat zpracovávané osobní údaje výhradně na šifrovaný externí hardware nebo software,
14. provádět průběžně ničení přípravných podkladů (rukopisů, konceptů, poznámek) sloužících ke zpracování za použití skartovacího stroje a softwarových prostředků,
15. pokud to informační systém elektronické spisové služby Organizace umožňuje, je oprávněná osoba povinna v rámci evidence v elektronické spisové službě povinna vést ve jmenném rejstříku veškeré subjekty údajů, jejichž osobní údaje jsou v evidovaném dokumentu zpracovávány.
16. Ostatní zaměstnanci organizace mimo oprávněné osoby
17. Zaměstnanci, kteří nejsou v postavení oprávněných osob, nejsou oprávněni zpracovávat osobní údaje.
18. Zaměstnanci jsou povinni dodržovat pravidla stanovená touto směrnicí, podrobnějšími pravidly vydanými vedoucím útvaru, nařízením GDPR a souvisejícími předpisy, a jednotlivé pokyny vedoucího útvaru.
19. Zaměstnanci jsou povinni zachovávat mlčenlivost o zpracovávaných osobních údajích (i v případě nahodile zpřístupněných údajů) a o implementovaných bezpečnostních opatřeních a zárukách k jejich ochraně. Povinnost mlčenlivosti trvá i po skončení pracovněprávního poměru či funkčního nebo smluvního vztahu k organizaci.
20. Zaměstnanci jsou povinni informovat bezodkladně vedoucího útvaru o jakémkoliv neoprávněném kontaktu s osobními údaji či v případě zjištěného úniku osobních údajů.
21. Vedoucí pozice:

Starosta(tka)

1. jmenuje pověřence pro ochranu osobních údajů,
2. ohlašuje pověřence na Úřadu pro ochranu osobních údajů,
3. zveřejňuje kontaktní údaje pověřence na webových stránkách úřadu,
4. zajistí, aby zaměstnanci organizace mohli s pověřencem konzultovat otázky zpracování a zabezpečení osobních údajů.

Vedoucí odboru a tajemník úřadu

1. průběžně kontroluje, zda jsou osobní údaje zpracovávány pouze na základě právních důvodů, pravidelně provádí kontrolu rozsahu zpracovávaných osobních údajů, dodržování účelu zpracování a přesnosti zpracování;
2. každoročně zajišťuje analýzu datových toků, funkčnosti využívaných prostředků při zpracování osobních údajů; obsahu interní dokumentace a smluv z úhlu pohledu zpracování a zabezpečení osobních údajů,
3. průběžně zabezpečuje informování subjektů údajů dle GDPR (informační povinnost správce dle čl. 13 a čl. 14 GDPR), a to sdělením těchto informací v jednotlivých formulářích, přihláškách, nebo na webových stránkách správce; průběžně kontroluje plnění informační povinnosti správce,
4. zajišťuje a kontroluje, aby byl souhlas se zpracováním osobních údajů využíván důvodně a nebyl nadužíván; aby byl souhlas se zpracováním osobních údajů poskytován jako svobodný, konkrétní a informovaný,
5. vede záznamy o činnostech zpracování (dle čl. 30 GDPR), průběžně je aktualizuje,
6. komunikuje s osobami nebo institucemi, které chtějí získat organizací zpracovávané osobní údaje; zejména tehdy, pokud je nutno ujasnit oprávnění osoby nebo organizace na získání osobních údajů; odesílá jménem organizace písemná hodnocení a posudky jiným subjektům (např. soudu),
7. zajišťuje proškolení zaměstnanců v oblasti zpracování osobních údajů, zajišťuje poučení zaměstnanců o právech a povinnostech při zpracování osobních údajů,
8. vyřizuje žádosti o výkon práv subjektů údajů v oblasti ochrany osobních údajů, příp. pověřuje zaměstnance, který se touto žádostí bude zabývat,
9. vyřizuje stížnosti subjektů údajů v oblasti ochrany osobních údajů,
10. zajišťuje obsahovou náplň smluv, jejichž plnění vyžaduje zpracování osobní údajů, která zajišťuje zabezpečení osobních údajů (tzn. smlouvy mezi správcem a zpracovatelem osobních údajů),
11. stanovuje okruh osob, které mají přístup do jednotlivých prostor, ve kterých se zpracovávají osobní údaje,
12. zajišťuje, aby měl každý zaměstnanec, který zpracovává citlivé osobní údaje v listinné podobě, k dispozici uzamykatelnou skříňku, resp. zásuvku,
13. stanoví pravidla evidence zpracování osobních údajů, zejména předávání dokumentů v listinné podobě, které obsahují osobní údaje,
14. stanoví pravidla ochrany osobních údajů v elektronické podobě,
15. stanoví pravidla odnášení z pracoviště pracovních notebooků obsahujících osobní údaje a práce na notebooku doma,
16. stanoví pravidla kopírování osobních údajů na externí nosiče,
17. stanoví pravidla likvidace vyřazených počítačových médií,
18. průběžně sleduje obsah vedené dokumentace vč. využívaného software, z úhlu pohledu důvodnosti a přesnosti zpracování osobních údajů, shromažďování osobních údajů na základě právního základu a v minimálním rozsahu; spolupracuje s tajemníkem a pověřencem na úpravě a aktualizace jím vedené dokumentace,
19. v případě zpracování osobních údajů v rámci působnosti daného útvaru na základě souhlasu subjektu údajů, odpovídá vedoucí tohoto útvaru za vedení evidence přijatých souhlasů subjektů údajů a kontrolu vedení této evidence.

Správce sítě, informatik zabezpečuje:

1. funkčnost systému,
2. technické zabezpečení sítě,
3. pravidelnou údržbu elektronického systému zpracování osobních údajů, zálohování a archivaci dat,
4. pravidelnou a efektivní antivirovou ochranu, zabezpečení znemožňující koncovým uživatelům instalovat software, který může být škodlivý,
5. specifikaci požadavků na fyzickou ochranu serverů a ostatních ICT zařízení,
6. podle pokynů tajemníka zaměstnancům zřizuje přístupové účty k datům a nastavuje zaměstnancům různé úrovně oprávnění při přístupu k datům,
7. přípravu likvidace vyřazených počítačových médií tak, aby byl znemožněn přístup k osobním údajům uložených na těchto médiích.

Část V. Zabezpečení osobních údajů

1. Účel a úrovně zabezpečení:
2. účelem zabezpečení osobních údajů je přijetí opatření a využití prostředků, kterými je zajištěna ochrana osobních údajů před zneužitím, ztrátou, poškozením osobních údajů a obnovitelnost dat;
3. zabezpečení osobních údajů probíhá na úrovni technické, organizační a personální.
4. Povinnosti zaměstnanců v souvislosti se zabezpečením osobních údajů

V souvislosti se zabezpečením osobních údajů jsou všichni zaměstnanci povinni dodržovat následující zásady zabezpečení osobních údajů:

1. vstupovat pouze do těch prostor, ve kterých se zpracovávají osobní údaje, do kterých jsou dle určení zaměstnavatele oprávněni vstupovat; vymezení těchto prostor je obsaženo v pracovní náplni zaměstnance, resp. vyplývá z jeho pracovního zařazení,
2. ukládat dokumenty obsahující citlivé osobní údaje v listinné podobě v uzamykatelných skříních, zásuvkách,
3. kopírovat osobní údaje na externí nosiče pouze tehdy, pokud to povolí vedoucí jeho útvaru,
4. účastnit se proškolení v oblasti zpracování osobních údajů,
5. při odchodu z pracoviště je nutné, aby veškeré dokumenty obsahující osobní údaje byly uklizené v prostorech k tomu určených,
6. zaměstnancům je zakázáno zejména nechávat třetí osoby samotné v kancelářích, kabinetech a jiných místnostech, kde jsou trvale uloženy dokumenty obsahující osobní údaje,
7. při zpracování osobních údajů v elektronické podobě dodržovat Bezpečnostní směrnici, zejména:
   * využívat pouze svého přístupového oprávnění, využívat hesla, automatické spořiče obrazovky,
   * odnášet notebooky obsahující osobní údaje z pracoviště a pracovat na notebooku doma pouze tehdy, pokud to povolí vedoucí jeho útvaru nebo tajemník; při práci s notebookem mimo pracoviště jsou zaměstnanci povinni zajistit, aby s notebookem nemanipulovaly jiné osoby,
   * používat ICT pouze k plnění svých pracovních povinností v souladu s účelem, ke kterému byly určeny,
   * přihlašovat se do počítače pod svým přihlašovacím jménem, příp. tokenem, a svým heslem, příp. PINem,
   * zdržet se instalací, aktualizací či oprav počítačových programů bez souhlasu správce sítě, resp. informatika. Všechny podstatné změny v nastavení softwaru provádí informatik,
   * zdržet se provádění instalace softwarových řešení, zejm. aplikací „zdarma“ na služební telefony či počítače; zaměstnanci, kteří využívají služební telefony nebo jsou oprávněni používat přenosné počítače mimo pracoviště, je nesmí „půjčovat“ třetím osobám, zejm. dětem,
   * pokud jsou zaměstnanci oprávněni odnášet si práci „domů“, např. na přenositelných discích, musí být tyto technologie chráněny; nelze ukládat a odnášet mimo pracoviště dokumenty s osobními údaji uložené např. na nezašifrovaných/nezaheslovaných flashdiscích,
   * zaměstnanci jsou povinni při odchodu z pracoviště (např. pauza na oběd) odhlásit se (např. klávesová zkratka Win+L), počítač zamknout nebo vypnout; při odchodu z pracoviště je vždy nutné počítač vypnout,
   * zaměstnanci, kteří se přihlašují přes tzv. token do počítače, jsou povinni při odchodu z pracoviště token vyjmout z přístroje a ponechat přes noc na zabezpečeném místě (např. v uzamykatelné skříňce v kanceláři); stejně tak je nutné při opuštění kanceláře (i na pět minut) kancelář uzamknout,
   * zaměstnanci, kteří k přístupu do počítače využívají uživatelské jméno a heslo, resp. PIN v případě využití tokenu, jsou povinni nastavit heslo, resp. PIN tak, že jednoduše nelze dojít k jeho prolomení a tedy, že účinně brání případným útokům; je zakázáno používat hesla shodná s přihlašovacím jménem, biografickými údaji (např. datum narození) apod.,
   * zaměstnancům je zakázáno otevírat podezřelé odkazy nebo přílohy e-mailů, v případě nejasnosti jsou povinni kontaktovat informatika,
   * zaměstnancům je zakázáno posílat dokumenty obsahující citlivé osobní údaje e-mailem, ledaže k tomu mají výslovný souhlas subjektu údajů.

Část VI. Smlouva se zpracovateli osobních údajů

1. Jestliže útvar z pozice správce osobních údajů předává osobní údaje ke zpracování za stanoveným účelem určitému zpracovateli, je povinen uzavřít s tímto zpracovatelem osobních údajů smlouvu o zpracování osobních údajů ve smyslu čl. 28 nařízení GDPR.
2. Jestliže útvar z pozice zpracovatele osobních údajů přebírá osobní údaje ke zpracování od správce osobních údajů nebo předává osobní údaje k dalšímu zpracování správci osobních údajů, je povinen uzavřít se správcem osobních údajů smlouvu o zpracování osobních údajů ve smyslu čl. 28 nařízení GDPR.
3. Potřebu uzavření smlouvy o zpracování osobních údajů a její obsah jsou útvary povinny konzultovat s pověřencem. Útvar je oprávněn k uzavření smlouvy o zpracování osobních údajů až po jejím odsouhlasení pověřencem a jejím schválení příslušným orgánem organizace.
4. Smlouva o zpracování osobních údajů musí mít písemnou formu. Může být uzavřena správcem a zpracovatelem jako součást jiné smlouvy (hlavní) nebo ve formě samostatné smlouvy.
5. Smlouva, k jejímuž plnění je nutné, aby smluvní strana nakládala s osobními údaji, musí obsahovat:
6. předmět a předpokládanou dobu zpracování osobních údajů,
7. povaha a účel zpracování osobních údajů,
8. typy (kategorie) zpracovávaných osobních údajů,
9. kategorie dotčených subjektů údajů,
10. povinnosti druhé smluvní strany

* přijmout konkrétně uvedená bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,
* nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu správce,
* zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
* zajistit, aby osoby oprávněné zpracovávat osobní údaje u zpracovatele byly zavázány k mlčenlivosti, a to i po skončení pracovněprávního poměru či funkčního nebo smluvního vztahu ke druhé smluvní straně, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
* zajistit, že zpracovatel bude správci bez zbytečného odkladu nápomocen při plnění povinností správce, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 GDPR, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 GDPR a povinnosti provádět předchozí konzultace dle čl. 36 GDPR, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje správce,
* po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí správci a vymaže existující kopie apod.,
* spolupracovat se správcem v tom smyslu, že poskytne správci informace potřebné k doložení toho, že byly splněny povinnosti stanovené správci právními předpisy, poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví správce, součinnost potřebnou pro plnění zákonných povinností správce spojených s ochranou osobních údajů, jejich zpracováním; umožnit kontrolu, audit či inspekci prováděné správcem nebo příslušným orgánem dle právních předpisů,
* poskytnuté osobní údaje chránit v souladu s právními předpisy,
* závazek úhrady škody způsobené Organizaci nedodržení povinností druhé smluvní strany a pokud s tím druhá strana bude souhlasit, specifikace pokuty za každý případ porušení v oblasti ochrany a zpracování osobních údajů.

Část VII. Posouzení vlivu na ochranu osobních údajů

1. Pokud je pravděpodobné, že určitý druh zpracování osobních údajů nespadající pod zákonné povinnosti organizace, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, je nutné provést před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.
2. Vedoucí útvaru je povinen, pokud se předmětné zpracování vztahuje k působnosti daného útvaru, informovat pověřence úřadu o každém zpracování osobních údajů, které podle názoru daného vedoucího útvaru vyžaduje posouzení vlivu dle předchozího odstavce.
3. Za zadání a provedení posouzení vlivu odpovídá tajemník, nebo jím pověřená osoba.
4. Posouzení vlivu musí být provedeno v souladu s nařízením GDPR (čl. 35 GDPR) a musí být posouzeno pověřencem podle čl. 35 odst. 2 nařízení GDPR.
5. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

Část VIII. Vznik nové činnosti zpracovávající osobní údaje

V případě, že v rámci útvaru vznikne nová činnost se zpracováním osobních údajů, je vedoucí útvaru, nebo jím pověřená osoba, před zahájením této činnosti povinen:

1. posoudit potřebu posouzení vlivu a příp. tuto konzultovat s pověřencem Organizace,
2. přidat popis činnosti do záznamů o činnostech zpracování daného útvaru a tento poskytnout k vyjádření pověřenci,
3. zajistit připravení formulářů a vzorů dokumentů pro zajištění této činnosti,
4. pro oprávněné osoby zajistit přístupová práva do informačních systémů, v rámci kterých budou osobní údaje zpracovávány,
5. v potřebném rozsahu zajistit uzamykatelné skříně pro ukládání listinných dokumentů s osobními údaji související s touto činností.

Část IX. Opatření pro zabezpečení osobních údajů

1. Základní personální opatření zabezpečení osobních údajů jsou následující:
2. Je zajištěno vstupní proškolení zaměstnanců v oblasti zpracování osobních údajů.
3. Každoročně je zajištěno proškolení zaměstnanců v oblasti zpracování osobních údajů. Toto proškolení organizuje odpovědný pracovník organizace.
4. Práva a povinnosti zaměstnanců spojená se zpracováním osobních údajů jsou systematicky zapracovávána do interních předpisů organizace a do pracovních náplní zaměstnanců.
5. Je zajištěna pravidelná konzultační činnost s pověřencem na úrovni vedení i na úrovni jednotlivých zaměstnanců.
6. Způsob zabezpečení elektronicky zpracovávaných osobních údajů je popsán v Bezpečnostní směrnici.
7. Listinné dokumenty obsahující osobní údaje jsou uloženy v uzamykatelných kancelářích, v případě zvláštních/citlivých osobních údajů navíc v uzamykatelných skříních v uzamykatelných kancelářích. V případě, že do kanceláře má přístup neoprávněná osoba v době nepřítomnosti oprávněné osoby (uklízečka, …), jsou listinné dokumenty obsahující osobní údaje uloženy v těchto kancelářích v uzamykatelných skříních/šuplících.
8. Bez souhlasu vedoucího útvaru nebo tajemníka nelze dokumenty obsahující osobní údaje vynášet z organizace, předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.
9. Spisy, které obsahují osobní údaje účastníků řízení a dalších osob, jsou uloženy v uzamykatelné skříni odděleně od jiné dokumentace. Přístup ke spisům mají pouze účastníci řízení nebo osoby jejichž právo přístupu vyplývá z platných zákonných ustanovení.
10. Zabezpečení osobních údajů uchazečů o zaměstnání a zaměstnanců
11. Dokumenty uchazečů o zaměstnání jsou uloženy v uzamykatelných skříních u zaměstnance odpovídajícímu za vedení Personální agendy po dobu vyplývající z některého titulu pro právní zpracování osobních údajů (zejména plnění zákonné povinnosti, nebo dle souhlasu subjektu údajů).
12. Do osobního spisu zaměstnance mají právo nahlížet vedoucí útvaru, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, v případě kontroly Úřad pro ochranu osobních údajů aj. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele.
13. Personální agenda (docházka) vedená v elektronické formě je vedena v zabezpečeném informačním systému. Do správy tohoto systému mají přístup pouze pověření zaměstnanci organizace.
14. Agenda účetní nebo mzdové účetní vedená v listinné podobě je uložena v uzamykatelné skříni v kanceláři mzdové účetní. Agenda účetní nebo mzdové účetní vedená v elektronické formě je vedena v zabezpečeném informačním systému. Do tohoto systému má přístup pouze účetní nebo mzdová účetní.

Část X. Porušení zabezpečení a hlášení porušení zabezpečení

1. Porušením zabezpečení se chápe takové porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
2. Každý zaměstnanec je povinen bez prodlení ohlásit jakékoli porušení zabezpečení osobních údajů tajemníkovi nebo jím pověřenému zaměstnanci, kteří neprodleně o této skutečnosti informují pověřence, se kterým konzultují další postup.
3. Pověřený pracovník organizace vždy zdokumentuje porušení zabezpečení osobních údajů. Dokumentace o porušení zabezpečení osobních údajů obsahuje
4. kdy k události došlo,
5. popis povahy daného případu porušení zabezpečení osobních údajů vč. č.j., kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
6. popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
7. popis postupu řešení vč. příp. opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných případných možných nepříznivých dopadů.
8. Pověřenec posoudí porušení zabezpečení a vyhodnotí, zda je pravděpodobné, nebo nepravděpodobné, že porušení zabezpečení bude mít za následek riziko pro práva a svobody subjektu fyzických osob.
9. V případě, že není pravděpodobné, že porušení zabezpečení bude mít za následek riziko pro práva a svobody fyzických osob, porušení zabezpečení osobních údajů správce nehlásí Úřadu pro ochranu osobních údajů. Každé porušení je však tajemníkem pověřený pracovník povinen interně zaznamenat a předložit v případě potřeby Úřadu pro ochranu osobních údajů.
10. V případě, že je pravděpodobné, že porušení zabezpečení bude mít za následek riziko pro práva a svobody fyzických osob, porušení zabezpečení osobních údajů správce hlásí prostřednictvím pověřence Úřadu pro ochranu osobních údajů, pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Pokud ohlášení Úřadu pro ochranu osobních údajů není učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
11. V případě, že je pravděpodobné, že porušení zabezpečení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, porušení zabezpečení osobních údajů správce oznamuje též dotčeným subjektům údajů, pokud je to technicky, nebo organizačně možné.
12. Opatření, které správce přijal k řešení porušení zabezpečení zpracovává zaměstnanec, do jehož činnosti porušení zabezpečení spadá, a schvaluje je tajemník.

Část XI. Pořizování kopií dokladů pro úřední potřeby organizace

Pořídit kopii dokladů subjektu údajů (občanského průkazu, cestovního dokladu, rodného listu, apod.) je možné pouze v případech nezbytných pro výkon konkrétní agendy, pokud je současně splněna jedna z následujících podmínek:

1. občan, kterému byl doklad vydán, poskytne útvaru organizace souhlas s pořízením jeho kopie pro konkrétní účel,
2. stanoví tak zvláštní právní předpis nebo mezinárodní smlouva, kterou je Česká republika vázána (např. dle § 22b zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů) a jedná se o výkon státní správy.
3. Ve zvláštních případech lze pořizovat kopie dokladů na základě povolení tajemníka úřadu.

Část XII. Předávání zpracovávaných osobních údajů do třetích zemí nebo mezinárodním organizacím

Zpracovávané osobní údaje mohou být předány útvary do třetí země (tj. nečlenského státu EU) nebo mezinárodní organizaci pouze po předchozím souhlasu pověřence a současně pouze za splnění některé z následujících podmínek vyplývajících ze čl. 45 až 50 nařízení GDPR:

1. Komise (EU) rozhodla, že tato třetí země nebo mezinárodní organizace zajišťují odpovídající úroveň ochrany osobních údajů,
2. správce nebo zpracovatel se sídlem v třetí zemi nebo mezinárodní organizace poskytly vhodné záruky odpovídající ochrany osobních údajů, případě včetně souhlasu Úřadu, nebo
3. jedná se o některou z výjimek stanovených výslovně v čl. 49 nařízení GDPR.

Část XIII. Práva subjektů údajů a informační povinnost správce

1. Plnění informační povinnosti vůči subjektům údajů dle čl. 13 a 14 nařízení GDPR zajišťují útvary, které osobní údaje získávají. Obecně je nutné plnit informační povinnost stručným, transparentním, srozumitelným a snadno přístupným, tedy vhodným způsobem za použití jasných a jednoznačných jazykových prostředků.

Informační povinnost vůči externím subjektům údajů je plněna primárně ve veřejně přístupné části webových stránek organizace. Zároveň je příslušný útvar povinen informovat subjekty osobních údajů ve chvíli získání osobních údajů o plnění informační povinnosti na těchto webových stránkách (např. na listinném formuláři příslušné agendy formou odkazu na příslušnou sekci internetových stránek).

Sekundárně lze plnit informační povinnost v rámci textu smluv uzavíraných se subjekty údajů nebo v rámci souhlasů se zpracováním osobních údajů poskytovaných subjekty údajů. Plnění informační povinnosti v uzavíraných smlouvách a poskytovaných souhlasech zajišťují jednotlivé útvary. Návrh textu ke splnění informační povinnosti projedná příslušný útvar s pověřencem.

Informační povinnost vůči zaměstnancům a veřejným funkcionářům Organizace je plněna primárně v rámci pracovních smluv nebo obdobných smluv u veřejných funkcionářů při jejich uzavírání a v rámci interních normativních aktů Organizace.

1. Společná pravidla pro vyřízení žádostí subjektů údajů

Tento odstavec upravuje společná pravidla pro vyřízení žádostí subjektů údajů podaných dle následujících odstavců „Přístup subjektů údajů k osobním údajům“ až „Právo vznést námitku“ v rámci tohoto článku této směrnice.

1. Postup přijetí žádosti subjektu údajů:

* Centrální podatelna, doručenou žádost v souladu se spisovým řádem zaeviduje do elektronického systému spisové služby a postoupí ji tajemníkovi nebo jím pověřené osobě k provedení dalších úkonů.
* Je-li žádost doručena žadatelem zástupci útvaru Organizace přímo (osobním doručením nebo prostřednictvím pošty), příslušný zástupce útvaru Organizace zkontroluje, zda-li je na žádosti subjekt údajů jednoznačně identifikován. V případě, že subjekt údajů jednoznačně identifikován není (např. jménem, příjmením, datem narození a adresou trvalého pobytu), upozorní subjekt údajů na tuto skutečnost a vyzve jej k doplnění této žádosti. Pokud subjekt údajů odmítne žádost doplnit, zástupce útvaru žádost od subjektu údajů převezme bez doplněné jednoznačné identifikace subjektu údajů. Následně zaměstnanec útvaru žádost bezodkladně zaeviduje v souladu se spisovým řádem a postoupí ji tajemníkovi, nebo jím pověřené osobě k provedení dalších úkonů.
* Je-li žádost subjektu údajů podána žadatelem ústně, požádá zástupce útvaru subjekt údajů k vytvoření písemné formy této žádosti, příp. s ním tuto žádost společně vytvoří dle požadavků subjektu údajů. Pokud subjekt údajů odmítne tuto žádost vytvořit písemnou formou, zástupce útvaru vytvoří záznam o podání této žádosti obsahující předané identifikační údaje žadatele a specifikaci vlastní žádosti včetně identifikace příp. přítomných svědků z řad zaměstnanců úřadu nebo zástupců obce. Dále s touto žádostí postupuje jako u předchozího odstavce (tj. jako by se jednalo o doručení žádosti žadatelem zástupci útvaru Organizace přímo).

1. Žádající subjekt údajů musí být řádně ztotožněn. Jednoznačné ověření totožnosti žadatele provede tajemník, nebo jím pověřena osoba. Podmínka jednoznačného ověření totožnosti žadatele je splněna v následujících případech:

* žádost byla podána prostřednictvím datové schránky žadatele,
* žádost byla podána prostřednictvím elektronické podatelny správce se zaručeným elektronickým podpisem žadatele,
* žádost byla podána v listinné podobě s úředně ověřeným podpisem žadatele,
* žadatel se osobně identifikoval správci předložením občanského průkazu, nebo cestovního dokladu. Takový způsob identifikace může být učiněn dotčeným útvarem při obdržení žádosti subjektu, o čemž je oprávněná osoba povinna učinit relevantní záznam na předmětné žádosti.

1. Pokud nebude možné provést na základě podané žádosti jednoznačné ověření totožnosti žadatele (nebude splněna žádná z podmínek uvedených v předchozím odst. b) této kapitoly, upozorní tajemník, nebo jím pověřená osoba, na tuto skutečnost žadatele v písemné formě do 10 kalendářních dnů ode dne obdržení jeho žádosti a sdělí mu, jakým způsobem naplnit podmínku jednoznačného ověření totožnosti žadatele.
2. Pokud není ze žádosti zřejmé, čeho se žadatel domáhá, upozorní tajemník, nebo jím pověřená osoba, na tuto skutečnost žadatele v písemné formě do 10 kalendářních dnů ode dne obdržení jeho žádosti a informuje ho o nutnosti upřesnění (doplnění) žádosti.
3. Tajemník, nebo jím pověřená osoba, je povinen zaslat žadateli odpověď na jeho žádost (resp. rozhodnutí o námitkách) do jednoho měsíce ode dne jejího obdržení.
4. Datum podání žádosti je den doručení žádosti do Organizace. Lhůta počíná běžet následujícím dnem od doručení žádosti. V případě podání žádosti prostřednictvím datové schránky anebo prostřednictvím elektronické adresy podatelny Organizace je podání učiněno okamžikem dodání zprávy do schránky Organizace, resp. den, kdy byla žádost doručena na elektronickou adresu podatelny Organizace.
5. Lhůtu 1 měsíce lze v případě potřeby z důvodu složitosti vyřízení žádosti nebo celkového počtu žádostí nejvýše dvakrát prodloužit, vždy nejvýše o další 1 měsíc (tj. celkově může lhůta činit nejvýše 3 měsíce). Tajemník, nebo jím pověřená osoba, je povinen o prodloužení lhůty včetně uvedení důvodu informovat žadatele, a to nejpozději do uplynutí původní lhůty pro vyřízení žádosti.
6. Pokud tajemník, nebo jím pověřená osoba, žádosti (námitkám) subjektu údajů nevyhoví, informuje (poučí) ho v odpovědi (rozhodnutí o námitkách) o jeho právu:

* na podání stížnosti k Úřadu dle čl. 77 nařízení GDPR, pokud se subjekt údajů domnívá, že zpracováním jeho osobních údajů je porušeno nařízení GDPR, a
* na soudní ochranu dle čl. 79 nařízení GDPR, pokud se domnívá, že jeho práva dle nařízení GDPR byla porušena v důsledku zpracování jeho osobních údajů v rozporu s nařízením GDPR.

1. Odpovědi na žádosti subjektu údajů jsou poskytovány subjektům údajů bezplatně. Tím není dotčen následující odst. j) této kapitoly směrnice.
2. V případě zjevně nedůvodné nebo nepřiměřené žádosti nebo subjektem údajů opakovaně podávané žádosti rozhodne tajemník, nebo jím pověřená osoba, v součinnosti s pověřencem o dalším postupu, přičemž zvolí dle skutkových okolností jednu z následujících možností:

* žádost standardně vypořádá bez uložení platby žadateli,
* žádost standardně vypořádá a uloží žadateli povinnost přiměřené platby zohledňující administrativní náklady spojené s vyřízením žádosti, nebo
* žádost bez věcného vypořádání odmítne (jako šikanózní).

1. Tajemník, nebo jím pověřena osoba, vede evidenci žádostí subjektů údajů.
2. Žádosti subjektu údajů včetně reakcí na tyto žádosti jsou zpracovávány do uzavření spisu a následně archivovány v souladu se Spisovým řádem úřadu.
3. Právo přístupu subjektů údajů k osobním údajům
4. Plnění povinnosti správce umožnit subjektu údajů na jeho žádost přístup k jeho osobním údajům dle čl. 15 nařízení GDPR zajišťuje tajemník, nebo jím pověřená osoba, v součinnosti s jednotlivými útvary a pověřencem.
5. V případě obdržení žádosti o přístup k osobním údajům bude žádost bezodkladně postoupena tajemníkovi, nebo jím pověřené osobě.
6. Tajemník, nebo jím pověřená osoba provede jednoznačné ověření totožnosti (identity) osoby žadatele, ledaže se žadatel osobně identifikoval na jiném útvaru.
7. Následně tajemník, nebo jím pověřená osoba, ve lhůtě stanovené touto směrnicí (viz. část VIII. odst. „2. Společná pravidla pro vyřízení žádostí subjektů údajů“ v tomto článku této směrnice) zašle žadateli odpověď na jeho žádost, ve které uvede následující informace:

* zda jsou osobní údaje žadatele správcem zpracovávány; pokud ano, pak dále uvede:
* účely zpracování,
* kategorie zpracovávaných osobních údajů,
* příjemce, kterým jsou zpracovávané osobní údaje zpřístupněny,
* plánovanou dobu, po kterou budou osobní údaje správcem zpracovávány,
* existenci práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektů údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování,
* právo podat stížnost u Úřadu proti konkrétnímu zpracování,
* veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů

a současně zašle kopie zpracovávaných osobních údajů žadateli (při první žádosti poskytne tyto kopie bezplatně, v případě dalších žádostí požaduje přiměřenou platbu na úhradu administrativních nákladů (např. náklady na tisk či pořízení nosiče).

1. Tajemník, nebo jím pověřená osoba, zašle informace ve shodné formě, v jaké byla žádost přijata (listinná nebo elektronická), ledaže žadatel ve své žádosti výslovně uvede, v jaké formě žádá odpověď poskytnout, nebo pokud by forma žadatele nezaručovala příjem zaslaných informací pouze žadatelem.
2. Ve výjimečných případech (např. když subjekt údajů není spokojen s odpovědí na žádost o přístup v tom znění, že o subjektu nejsou zpracovávány žádné osobní údaje, přestože subjekt údajů má např. rozhodnutí Organizace v jeho věci) je možné odůvodnit neposkytnutí požadovaných osobních údajů subjektu údajů, resp. rozhodnutí o odmítnutí žádosti, například textem: „Údaje zpracovávané o Vaší osobě nebylo možné vyhledat při vynaložení přiměřeného úsilí a zohlednění použitých prostředků, nákladů a času tak, aby byl splněn účel práva na přístup dle čl. 15 nařízení GDPR. Z tohoto důvodu považujeme Vaši žádost ve zbylém rozsahu za nepřiměřenou ve smyslu čl. 12 odst. 5 nařízení GDPR.“, nebo „Vámi požadované informace jsou jednak zpracovávány ve výše uvedeném rozsahu, další případně zpracovávané údaje nebylo možné vyhledat při vynaložení přiměřeného úsilí a zohlednění použitých prostředků, nákladů a času tak, aby byl splněn účel práva na přístup dle čl. 15 nařízení GDPR. Z tohoto důvodu považujeme Vaši žádost ve zbylém rozsahu za nepřiměřenou ve smyslu čl. 12 odst. 5 nařízení GDPR.“
3. Právo subjektu údajů na opravu osobních údajů
4. Plnění povinnosti správce provést opravu nepřesně zpracovávaného osobního údaje nebo doplnění neúplně zpracovávaných osobních údajů dle čl. 16 nařízení GDPR zajišťují jednotlivé útvary v součinnosti s tajemníkem nebo jím pověřeným pracovníkem a pověřencem.
5. V případě obdržení žádosti o opravu nesprávně nebo neúplně zpracovávaných osobních údajů bude žádost bezodkladně postoupena tajemníkovi nebo jím pověřenému pracovníkovi a pověřenci.
6. Tajemník nebo jím pověřený pracovník provede jednoznačné ověření identity osoby žadatele ve smyslu této směrnice, ledaže se žadatel osobně identifikoval na jiném útvaru.
7. Tajemník nebo jím pověřený pracovník v součinnosti s jednotlivými útvary a případně s pověřencem posoudí důvodnost žádosti žadatele (tj. zda jsou jeho osobní údaje skutečně nesprávně nebo neúplně zpracovávány).
8. Pokud není žádost shledána důvodnou, zašle tajemník nebo jím pověřený pracovník ve lhůtě stanovené touto směrnicí (viz. část VIII. odst. „2. [Společná pravidla pro vyřízení žádostí subjektů údajů](#_Společná_pravidla_pro)“ tohoto článku této směrnice) odpověď obsahující informaci o nevyhovění žádosti včetně odůvodnění žadateli.
9. Pokud je žádost shledána důvodnou, zašle tajemník nebo jím pověřený pracovník ve lhůtě stanovené touto směrnicí (viz. část VIII. odst. „2 [Společná pravidla pro vyřízení žádostí subjektů údajů](#_Společná_pravidla_pro)“ tohoto článku této směrnice) odpověď obsahující informaci o vyhovění žádosti žadateli a provede v součinnosti s příslušnými útvary opravu (doplnění) zpracovávaných osobních údajů.
10. Právo subjektu údajů na výmaz osobních údajů
11. Útvary provádí průběžně výmaz zpracovávaných osobních údajů, jestliže nastane některý z následujících důvodů:

* osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
* subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní titul pro zpracování,
* subjekt údajů vznese námitky proti zpracování podle čl. 15 této směrnice a neexistují žádné převažující oprávněné důvody pro zpracování,
* správce zjistí, že osobní údaje byly zpracovány protiprávně,
* povinnost výmazu osobních údajů stanoví právní řád,
* osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 nařízení GDPR, a správce zjistí, že dítě poskytující souhlas nedosáhlo v okamžiku poskytnutí souhlasu 15 let věku.

1. Útvary nejsou povinny osobní údaje bez ohledu na předchozí odst. a) této směrnice vymazat, pokud je zpracování nezbytné:

* pro výkon práva na svobodu projevu a informace,
* pro splnění právní povinnosti, jež vyžaduje zpracování podle právního řádu nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
* z důvodů veřejného zájmu v oblasti veřejného zdraví ve smyslu čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 nařízení GDPR,
* pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 nařízení GDPR, pokud je pravděpodobné, že by výmaz osobních údajů znemožnil nebo vážně ohrozil splnění cílů uvedeného zpracování,
* pro určení, výkon nebo obhajobu právních nároků správce.

1. Výmaz osobních údajů je vždy možné provést teprve po uplynutí skartačních lhůt dokumentů a jejich zařazení do procesu výběru archiválií, a to pouze u těch dokumentů, které nebudou příslušným archivem vybrány jako archiválie dle zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů.
2. Právo subjektu údajů na omezení zpracování osobních údajů
3. Subjekt údajů má právo, aby správce omezil zpracování jeho osobních údajů, pokud nastane některý z následujících důvodů:

* subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit,
* zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití,
* správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,
* subjekt údajů vznesl námitku proti zpracování dle této směrnice, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

1. Pokud bylo zpracování omezeno podle předchozího odst. 6 písm. a) , mohou být osobní údaje, s výjimkou jejich uložení, nadále správcem 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 důvodu důležitého veřejného zájmu.
2. Ustanovení odst. „Právo subjektu údajů na opravu osobních údajů“ tohoto článku této směrnice se pro omezení zpracování osobních údajů použijí obdobně.
3. Tajemník, nebo jím pověřena osoba, je povinen subjekt údajů předem upozornit o plánovaném zrušení omezení zpracování osobních údajů.
4. Právo subjektu údajů na přenositelnost osobních údajů
5. Právo na přenositelnost zpracovávaných osobních údajů je subjekt údajů oprávněn uplatnit u správce za kumulativního splnění následujících podmínek:

* osobní údaje poskytl správci sám subjekt údajů,
* zpracování není prováděno z titulu plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
* zpracování je založeno na právním titulu souhlasu subjektu údajů, nebo na právním titulu plnění smlouvy (viz. odst. „Právní důvod zpracování osobních údajů“ této směrnice), a
* zpracování se provádí u správce automatizovaně.

1. Pokud jsou splněny podmínky stanovené v předchozím odst. 7 písm. a) , je subjekt údajů oprávněn požádat správce o poskytnutí těchto osobních údajů ve strukturovaném, běžně používaném a strojově čitelném formátu, nebo o jejich přímé předání jinému správci určenému subjektem údajů. K přímému předání osobních údajů jinému správci je správce povinen pouze, pokud je to technicky proveditelné.
2. Ustanovení odst. „Právo subjektu údajů na opravu osobních údajů“ tohoto článku této směrnice se pro přenositelnost osobních údajů použijí obdobně.
3. Pokud je žádost shledána důvodnou, zašle tajemník, nebo jím pověřená osoba, ve lhůtě dle směrnice (viz. část VIII. odst. „2 Společná pravidla pro vyřízení žádostí subjektů údajů“ tohoto článku této směrnice) odpověď obsahující informaci o vyhovění žádosti žadateli a provede přenos zpracovávaných osobních údajů žadateli nebo na základě jeho požadavku jinému správci.
4. Právo subjektu údajů vznést námitku
5. Subjekt údajů má právo vznést námitku proti zpracování osobních údajů založených na právních titulech plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen, nebo ochraně práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby (viz. odst. „[Právní důvod zpracování osobních údajů](#_Právní_důvod_zpracování)“ této směrnice).
6. Správce je povinen, v případě zpracování osobních údajů pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci a zpracování osobních údajů jako oprávněný zájem správce (viz odst. „[Právní důvod zpracování osobních údajů](#_Právní_důvod_zpracování)“ této směrnice), informovat subjekt údajů o právu vznést proti takovému zpracování námitky, a to nejpozději při zahájení zpracování osobních údajů. Tato informace se standardně poskytuje v rámci informační povinnosti správce.
7. Tajemník, nebo jím pověřená osoba v součinnosti s jednotlivými útvary a pověřencem posoudí oprávněnost doručených námitek. Námitky jsou oprávněné, pokud správce zpracovává osobní údaje na základě právních titulů specifikovaných v předchozím odst. b) a neprokáže existenci závažných oprávněných důvodů pro takové zpracování ležících na své straně, které převažují nad zájmy (právy a svobodami) subjektu údajů na ochranu jeho osobních údajů, nebo neprokáže, že je takové zpracování nezbytné pro určení, výkon nebo obhajobu jeho právních nároků.
8. Tajemník, nebo jím pověřená osoba ve lhůtě dle této směrnice (viz. část VIII. odst. „2 [Společná pravidla pro vyřízení žádostí subjektů údajů](#_Společná_pravidla_pro)“ tohoto článku této směrnice) zašle odpověď s odůvodněním žadateli a pokud jsou námitky shledány jako oprávněné, zajistí v součinnosti s příslušnými útvary výmaz zpracovávaných osobních údajů.
9. Ustanovení odst. „Právo subjektu údajů na opravu osobních údajů“ tohoto článku této směrnice se pro právo vznést námitku použijí obdobně.

Část XIV. Spolupráce s pověřencem

1. Pověřenec je fyzická nebo právnická osoba, která má odborné znalosti a zkušenosti v oblasti právní úpravy zpracování osobních údajů, v oblasti informačních technologií, managementu a provozu organizace. Pokud je pověřencem právnická osoba, vykonává činnost pověřence fyzická osoba, zpravidla její zaměstnanec.
2. Pověřenec je určen starostou obce, kterému je i podřízen. Pověřenec vykonává činnost na základě pracovní smlouvy, dohody o pracovní činnosti nebo smlouvy o poskytování služeb.
3. Pověřenec přímo a pravidelně spolupracuje s tajemníkem úřadu.

V určenou dobu může s pověřencem konzultovat otázky zpracování osobních údajů a zabezpečení osobních údajů jakýkoli zaměstnanec organizace.

1. Úkoly pověřence:

Ve spolupráci s vedením organizace pověřenec

* soustavně sleduje soulad činností organizace s pravidly stanovenými GDPR a dalšími právními předpisy upravujícími zpracování osobních údajů;
* pravidelně analyzuje zjištění o zpracování osobních údajů v organizaci a zabezpečení osobních údajů v organizaci;
* upozorňuje na potenciální rizikové faktory v oblasti zpracování osobních údajů a jejich zabezpečení;
* informuje o postupech, které jsou v souladu s GDPR; navrhuje řešení a postupy při zpracování osobních údajů a zabezpečení osobních údajů;
* podílí se na pravidelném proškolení zaměstnanců a na vstupním proškolení nových zaměstnanců v oblasti ochrany osobních údajů a jejich zabezpečení;
* spolupracuje s Úřadem pro ochranu osobních údajů;
* poskytuje poradenství v souvislosti s povinností posouzení vlivu na ochranu osobních údajů.

1. Práva pověřence

* pověřenec má oprávnění k přístupu ke všem systémům organizace, pomocí kterých se zpracovávají osobní údaje;
* v rámci plnění svých úkolů má pověřenec právo na účinnou a efektivní spolupráci zaměstnanců organizace.

Část XV. Závěrečná a přechodná ustanovení

* + - 1. Tato směrnice byla schválená na 15. schůzi Rady města Humpolec dne   
         26. července 2023 pod číslem usnesení xxx/15/RM/2023 a nabývá účinnosti dne   
         1. srpna 2023.
      2. Touto směrnicí se zrušuje směrnice č. 1/2015, upravující nakládání s osobními údaji u Městského úřadu Humpolec ze dne 1. února 2015.

V Humpolci, 26. července 2023

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mgr. Alena Štěrbová, starostka města Mgr. Jiří Fiala, tajemník MěÚ