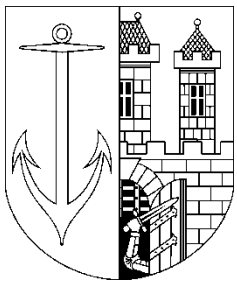
;



Městská část Praha 7 **tajemník ÚMČ Praha 7**

NAŘÍZENÍ

tajemníka č. 2 ze dne 25.05.2018
s účinností od 25.05.2018

Informační systémy, zpracování osobních údajů a jejich ochrana

1. Účel

1. Úřad Městské části Praha 7 (dále "úřad" nebo "ÚMČ P7") vykonává agendy, jejichž součástí je zpracování[1] dat[2]. Informační systém úřadu (IS) jsou nástroje a služby určené pro toto zpracování.
2. Účel tohoto dokumentu je zajištění kromě jiného těchto *funkcí* úřadu:
   - Zpracování dat probíhá v souladu se všemi relevantními legislativními opatřeními – zejména Zákon o ochraně osobních údajů[3] a GDPR[4].
   - IS nebo jeho libovolná část nebo data jsou chráněny před neautorizovaným přístupem.
   - Zpracování dat se děje pouze v rámci agend vykonávaných úřadem.
   - Informace v IS jsou zajištěny, aby byly přesné, důvěrné a dostupné.
   - Zpracování dat je možné nepřetržitě (s ohledem na pracovní dobu).
3. Tento dokument popisuje IS (viz 2. Informační systém) a jeho pravidla (viz 3. Pravidla pro užívání IS), a pravidla pro 4. Zpracování osobních údajů.

2. Informační systém

1. Uživatel IS (dále "uživatel") je osoba, která může používat jakoukoli část IS.
2. Uživatelům jsou k dispozici nástroje a služby IS uvedené v této kapitole.

2.1. HelpDesk

1. HelpDesk je aplikace pro evidenci požadavků ohledně fungování IS, dostupná na adrese:
   http://p7swap1/hesk (http://P7helpdesk)
2. Pokud požadavek není evidován v HelpDesku, IT nemá povinnost se jím zabývat. Ve výjimečných případech (kdy např. nelze zapnout PC, nebo krizové situace) je možné s IT komunikovat pomocí emailu, telefonicky nebo osobně.

---

[1] Shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace

[2] Data (údaje) *reprezentují* informace. Např. posloupnost znaků: v ě k 2 5 l e t jsou *data*, která reprezentují informaci: *[Osoba] ve věku dvaceti-pěti let.* Data mohou mít podobu písemnou, obrazovou, zvukovou, kombinovanou. Podle druhu média, které data nese, lze uvažovat data fyzická a elektronická.

[3] Zákon 101/2000Sb., o ochraně osobních údajů

[4] Nařízení Evropského parlamentu a rady (EU) 2016/679

2.2. Vzdálená podpora

1. Uživatelská podpora je k dispozici i vzdáleně – IT se připojí na pracovní plochu počítače uživatele a provede požadovanou operaci. Nástrojem pro vzdálenou podporu je aplikace TeamViewer.
2. IT provádí tento způsob podpory pouze se souhlasem uživatele.

2.3. Počítač

1. Osobní počítač třídy PC s operačním systém Windows – k dispozici jako:
   - Desktop – stolní počítač
   - Notebook – přenosný počítač
   - Tablet
2. Desktop mají k dispozici všichni uživatelé.
3. Notebook nebo Tablet je uživatelům k dispozici po schválení vedoucím odboru a tajemníkem úřadu.
4. Uživatel musí Notebook pravidelně a na dostatečně dlouhou dobu připojovat k internetu, aby byly aktualizovány funkce a zabezpečení Notebooku (operační systém a ostatní programové vybavení).
5. Přístup k počítači má uživatel neustále pod kontrolou. V případě, že se uživatel vzdálí od počítače, je povinen počítač uzamknout:
   - Stiskem kláves CTRL+ALT+DEL –> ENTER
   - Stiskem kláves WINDOWS+L
   - Odhlášením ze systému

2.4. Mobilní telefon

1. Mobilní telefon s určitým hlasovým a datovým tarifem s parametry podle aktuální smlouvy s operátorem.
2. Uživatel má přístup k mobilnímu telefonu neustále pod kontrolou. Telefon je zabezpečen[5] proti přístupu jinými osobami než uživatel.

2.5. Elektronická pošta

1. Schránka elektronické pošty a kalendář jsou dostupné pomocí aplikace Outlook.
2. Schránka a kalendář jsou dostupné pomocí webového rozhraní odkudkoli z internetu na adrese:

   https://posta.praha7.cz

[5] Např. heslem nebo biometrickou identifikací.

3. Pro služební účely lze používat pouze elektronickou poštu, která je součástí IS.
4. Příchozí pošta, vyhodnocená jako spam, je zadržena. O její doručení lze požádat IT.

2.6. Internet a VPN

1. Připojení k internetu je dostupné všem uživatelům IS.
2. Uživatel může IS používat prostřednictvím VPN – připojené zařízení se stane součástí IS jako kdyby se fyzicky nacházelo v budovách úřadu.
3. Internetová komunikace může být omezena nebo monitorována.

2.7. Úložný prostor

1. Osobní úložný prostor je na disku Q.
2. Sdílený úložný prostor je na discích R a X.
3. Disky Q, R, X jsou zálohovány.
4. Úložný prostor na lokálních discích počítače (typicky C, D, …) není zálohován a jeho používání je na vlastní riziko uživatele. Uživatel je povinen ukládat pracovní data pouze na zálohovaných discích.

2.8. Tisk a kopírování

1. Pro tisk a kopírování dokumentů jsou v IS dostupné tiskárny a kopírky.
2. Nepotřebné výtisky je nutno skartovat.

2.9. Elektronický podpis

1. Elektronické dokumenty lze opatřovat elektronickým podpisem.
2. Certifikát, nezbytný pro funkci elektronického podpisu, dostane uživatel na základě odůvodněné žádosti příslušného vedoucího odboru. Žádost lze podat až po uplynutí zkušební doby uživatele.
3. Vlastník certifikátu je povinen s certifikátem zacházet tak, že pravděpodobnost kompromitace certifikátu je minimální. V případě podezření na kompromitaci certifikátu (např. certifikát byl odcizen), je uživatel povinen tuto situaci nahlásit IT (viz 2.1. HelpDesk), který certifikát zneplatní.
4. Při rozvázání pracovního poměru zajistí IT zneplatnění daného certifikátu na základě Výstupního listu (viz příloha Výstupní list).

2.10. Zálohování dat

1. Zálohování dat v úložištích (viz 2.7. Úložný prostor) se děje 1 x za den bez nutnosti intervence uživatelů.
2. Data v aplikacích (viz 2.14. Aplikace) jsou průběžně zálohována bez nutnosti intervence uživatelů.
3. Obnovení dat probíhá na základě žádosti adresované IT (viz 2.1. HelpDesk).

2.11. Antivirová ochrana

1. Na počítačích běží antivirový program s cílem minimalizovat pravděpodobnost kontaminace IS škodlivým kódem.
2. Účinnost antivirové ochrany není 100 % a proto se uživatelé chovají obezřetně při nakládání s daty z neznámých zdrojů.
3. V případě podezření na virovou nákazu uživatel situaci neprodleně hlásí IT (viz 2.1. HelpDesk).
4. Jakýkoli přenosný nosič informací (CD, DVD, USB flash disky a pod.) musí uživatel před použitím proskenovat antivirovým programem, aby zajistil minimální pravděpodobnost kontaminace IS škodlivým kódem.

2.12. Anonymizace dokumentů

1. Pro anonymizaci dokumentů je k dispozici Adobe Reader.

2.13. Docházka

1. V aplikaci Docházka se eviduje přítomnost zaměstnanců na pracovišti.
2. Evidence vzniká použitím čipové karty u terminálů, případně na adrese: http://10.38.2.4/dochazka
3. Zaměstnanci jsou povinni evidovat svoji přítomnost na pracovišti (viz pracovní řád).

2.14. Aplikace

1. Součástí IS jsou aplikace pro vedení agend. Jedná se například:
   - E-spis (elektronický systém spisové služby)
   - Ginis (finanční a ekonomické záležitosti)
   - AiP Safe (dokumenty pro zastupitelstvo a radu)
   - IDES (evidence nemovitostí)
   - Vita (evidence přestupků)
   - Datacentrum Personalistika (personální evidence)
   - Datacentrum Docházka (evidence docházky)

3. Pravidla pro užívání IS

1. Pravidla zde uvedená platí pro každého uživatele IS. Jejich porušení může být považováno za porušení pracovní kázně se všemi pracovně právními následky.
2. V případě ohrožení zdraví nebo majetku některá zde uvedená pravidla neplatí.
3. Přístup k IS vzniká a zaniká podle pravidel v kap. 3.1. Přístup k IS.

4. Uživatelé jsou oprávněni používat IS nebo libovolnou část IS pouze v rámci agend vykonávaných úřadem. Jiné použití IS (zejména pro soukromé účely) je zakázáno.
5. Uživatelé nakládají s IS a jeho částmi hospodárně.
6. IS a veškerá data v něm obsažená jsou majetkem úřadu.
7. Fungování IS zajišťuje Odbor Informačních technologií (dále "IT").
8. Dostupnost IS je garantována v pracovní době.
9. Veškeré změny[6] v IS provádí výhradně IT. Ostatním uživatelům je zakázáno provádět jakékoliv změny v IS.
10. Uživatelé jednají tak, že je vyloučena možnost porušení některé *funkce* uvedené v kap. 1. Účel.
11. Uživatelé jsou povinni zachovávat mlčenlivost o všech získaných informacích.
12. Jakoukoli poruchu IS, případně podezření na riziko, které by mohlo vést k ohrožení některé *funkce* uvedené v kap. 1. Účel, je uživatel povinen nahlásit IT (viz 2.1. HelpDesk). Mezi poruchy nebo rizika může patřit:
    - Uživatel zjistí, že on nebo jiný uživatel má přístup k části IS nebo datům, ke kterým by přístup mít neměl.
    - Podezření na dokumenty (včetně emailů), které by mohly obsahovat škodlivý kód.
13. Uživatelé jsou povinni umožnit IT přístup ke svým počítačům a na vyžádání s IT spolupracovat.
14. IS nebo jeho libovolná část může být monitorována.
15. Uživatelé jsou povinni zálohovat data důležitá pro vykonávání agend úřadu v případech, kdy tato data nebyla zálohována jiným způsobem.
16. Je zakázáno používat soukromá paměťová média (např. USB / flash disky) pro ukládání pracovních dat.

3.1. Přístup k IS

1. Osoba se stane uživatelem IS přidělením přístupu do IS.
2. Rozsah přístupu nastavuje IT na základě žádosti vystavené vedoucím odboru a zaslané IT (viz 2.1. HelpDesk).

[6] Jakékoli zásahy do fyzických nebo programových vrstev IS.

3. U nového zaměstnance je součástí žádosti "Vstupní list" (viz. Příloha č. 1), který vystavuje Odbor personálních činností. Vedoucí odboru doplňuje rozsah přístupu (agendy), do kterých má mít nový zaměstnanec přístup.
4. Vedoucí odboru zodpovídá za rozsah přístupu uživatele.
5. Přístup do domény IS (přihlášení k počítači) umožňuje uživatelské *jméno* a *heslo*.
6. *Heslo* si uživatel pouze *pamatuje*, nikam ho neukládá, nezapisuje a nikomu nesděluje. Heslo lze v případě potřeby sdělit určenému zástupci.
7. Heslo se mění po stisku kláves CTRL+ALT+DEL volbou "změnit heslo" nebo po vypršení jeho platnosti (obvykle 180 dní).
8. Vlastnosti přijatelného hesla[7] se uživatel dozví z informací na monitoru při změně hesla.
9. Při ukončení pracovního poměru se zaměstnancem vedoucí odboru odešle IT žádost (viz 2.1. HelpDesk) o zrušení přístupů do IS. Součástí žádosti je vyplněný Výstupní list (viz Příloha č. 2). IT zodpovídá za to, že všechny přístupy daného zaměstnance budou zneplatněny nejpozději k datu uvedenému ve Výstupním listu.
10. Externí uživatel[8] je osoba, která má přidělen zvláštní režim přístupu do IS. Externí uživatel je např. zástupce dodavatele informačních technologií, který přístup používá pouze při servisních zásazích v IS a to vždy za přítomnosti pracovníka IT, nebo dle dané servisní smlouvy.

3.2. IT

1. Zálohuje infrastrukturu IS tak, aby byla minimalizována pravděpodobnost, že dojde k omezení schopnosti úřadu vykonávat jeho agendy. Zejména:
   - Zálohuje systém elektronické pošty.
   - Zálohuje data na úložištích (viz 2.7. Úložný prostor).
   - Zálohuje data v aplikacích a aplikace samotné.
   - Zajišťuje náhradní zdroj napájení pro některé části IS.
2. Analyzuje dopady plánovaných změn v IS a vytváří strategie, které minimalizují jejich možný negativní dopad.
3. Jednou ročně provede audit přístupů do IS.
4. Nejméně 1x za půl roku provádí audit nainstalovaného SW a kontrolu licencí.
5. V případě, že kontrola nad částí IS přechází na jiný subjekt než úřad, IT zajistí neobnovitelnou destrukci dat v dané části IS.
6. Odpovídá za to, že vztah (smlouva) s externími uživateli IS je v souladu s GDPR[9].

[7] Minimální délka 8 znaků, alespoň jedno malé písmeno, alespoň jedno velké písmeno, alespoň jedna číslice, alespoň jeden speciální znak.
[8] Např. dodavatel části IS.
[9] Nařízení Evropského parlamentu a rady (EU) 2016/679

3.3. Licence

1. Zaměstnanec nesmí používat, či poskytnout jiným uživatelům, jakékoliv neoprávněně získané klíče, sériová čísla či jiné technické prostředky sloužící k zajištění informační bezpečnosti a ochraně počítačových programů.
2. Zaměstnanec nesmí odstranit jakékoliv informace, označení či zařízení identifikující nositele či vykonavatele autorských práv k počítačovým programům, autora či jinou oprávněnou osobu.
3. Instalace a užívání nelegálního nebo neschváleného SW je považováno za hrubé porušení pracovní kázně. Za případné trestněprávní důsledky, které vyplynou z užívání nelegálního SW, nese plnou odpovědnost uživatel.

3.4. Opuštění pracoviště

1. Uživatel, který opouští pracoviště jako poslední, je povinen daný prostor zabezpečit proti přístupu neoprávněných osob.
2. Zaměstnanec odpovídá za to, že na pracovišti nebudou ponechána volně přístupná data (listinná nebo elektronická) služebního charakteru ani data nebo software neslužebního charakteru.

4. Zpracování osobních údajů

1. Úřad MČ Praha 7 je ve smyslu GDPR[10] správce[11] a zpracovatel[12] osobních údajů. Osobní údaje (OÚ) jsou data, která reprezentují informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů (SÚ) je fyzická osoba, k níž se osobní údaje vztahují. Zpracování osobních údajů je jakákoliv operace[13] nebo soustava operací systematicky prováděná s osobními údaji.
2. Pověřenec pro ochranu osobních údajů (pověřenec) je funkce, která dohlíží, aby zpracování OÚ úřadem bylo v souladu s GDPR. Pověřenec průběžně analyzuje zpracování OÚ na úřadu. Na základě analýzy navrhuje tajemníkovi, IT a vedoucím odborů opatření, aby zpracování osobních údajů bylo v souladu s GDPR. Kontaktní údaje na pověřence jsou uvedeny na webových stránkách úřadu.
3. Ke zpracování OÚ může docházet na základě souhlasu SÚ nebo zákonného důvodu.
    - Vzor souhlasu je v příloze Souhlas se zpracováním OÚ. Konkrétní znění souhlasu je nutné konzultovat s pověřencem. Osoba odpovědná za zpracování OÚ založeného na souhlasu SÚ musí být schopna prokázat, že SÚ vyjádřil s danou operací zpracování souhlas.

[10] Nařízení Evropského parlamentu a rady (EU) 2016/679

[11] Každý subjekt, který určuje účel a prostředky zpracování osobních údajů.

[12] Každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje.

[13] Shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

- Zákonným důvodem je:
  - Dodržení právní povinnosti.
  - Nezbytnost pro plnění smlouvy se SÚ.
  - Ochrana zájmů SÚ, nebo jiné fyzické osoby.
  - Veřejný zájem, výkon veřejné moci.
  - Oprávněné zájmy úřadu.

4. Úřad pro každé zpracování OÚ vede (písemně, včetně elektronické formy) tzv. záznamy o zpracování OÚ (záznamy o zpracování). Za vedení záznamů odpovídá pověřená osoba za danou agendu. Úřad je povinen poskytnout záznamy na požádání dozorového úřadu.[14] Součástí záznamů o zpracování je:
   - Jméno a kontaktní údaje úřadu a pověřence
   - Účely zpracování
   - Základ zpracovaní (souhlas SÚ nebo zákonný důvod)
   - Popis kategorií subjektů údajů
   - Popis kategorií osobních údajů
   - Způsob zpracování[15]
   - Pravidla (např. interní pracovní směrnice)
   - Odpovědná osoba
   - Rizikovost
   - Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích
   - Informace o předání OÚ do třetí země
   - Je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů
   - Je-li to možné, popis technických a organizačních opatření k zabezpečení údajů
5. Neúčelné zpracování není dovoleno. Účel musí být stanoven před zahájením zpracování. Sekundární užití údajů za jiným účelem vyžaduje nový právní důvod.
6. Při transferu údajů třetím osobám musí být nově stanoven účel a právní důvod.
7. Veškeré zpracování OÚ se řídí obecnou zásadou *minimalizace* zpracování. Údaje se zpracovávají pouze v nezbytném rozsahu. Např. pokud jsou údaje uloženy v aplikaci nebo databázi, není žádoucí, aby byly ukládány navíc v souborech na úložištích IS, na přenosných médiích, nebo v elektronické poště.
8. Při podezření, že došlo k porušení zabezpečení osobních údajů, je uživatel povinen neprodleně informovat pověřence. Pověřenec má pro další postup k dispozici lhůtu 72 hodin.

[14] Úřad pro ochranu osobních údajů
[15] např. listinná, elektronická, hybridní forma.

9. Zpracováním OÚ může úřad pověřit zpracovatele – externí subjekt. V takovém případě zpracování OÚ probíhá pouze na základě smlouvy nebo dodatku ke smlouvě, která je v souladu s GDPR.
10. Postup při vyřizování žádostí subjektů údajů ve smyslu GDPR:
    - Doručený dokument s žádostí je z podatelny předán pověřenci.
    - Pověřenec předá žádost (případně její části) na jednotlivé vedoucí odborů.
    - Vedoucí odborů poskytnou pověřenci informace relevantní k žádosti v takové lhůtě, aby žadatel obdržel odpověď nejpozději v zákonné lhůtě 30 dnů od podání žádosti.
    - Pověřenec vyřídí odpověď na žádost.

Mgr. Radomír Špok v.r.
tajemník Úřadu MČ Praha 7

„ otisk úředního razítka“

Příloha č. 1

VSTUPNÍ LIST NOVÉHO ZAMĚSTNANCE	
Jméno a příjmení	
Osobní číslo	
Pracovní zařazení	
Odbor/útvar	
Datum nástupu	
POŽADAVKY NA ZAJIŠTĚNÍ PRACOVNÍCH PODMÍNEK NOVÉHO ZAMĚSTNANCE	
Informatika	
Pracovní pozice	**Po kom nový zaměstnanec nastupuje/nová pozice**
GINIS + název modulu (ano - modul UCR,SML atd.)	
přístup do základních registrů a rozsah oprávnění ROB, ROS, RUIAN, RPP (certifikáty se vystavují až po zkušební době)	
e - spis/funkční místo (ano - například ORZ_REF4)	
přístup do Codexis (ano/ne)	
přístup do jiné aplikace (OKnouze, ENO, EVI, Misys atd…)	
AIP safe + členství ve skupinách (ano - například DMS.Uzivatel)	
notebook (ano/ne)	
Další vybavení (například scanner…)	
Provozní oddělení KST	
mobilní telefon	ano/ne
aktivace	ano/ne
datové služby	ano/ne
ochranné pracovní prostředky	
školení řidičů referentských vozidel	ano/ne
Personalistika/vzdělávání	
vstupní školení	
zkoušky odborné způsobilosti	
jiné školení	
Jiné požadavky - specifikovat	
V Praze dne:	
Navrhl:	Schválil: Mgr. Radomír Špok, tajemník ÚMČ P7

Příloha č. 2

Výstupní list
(pro zrušení přístupu do IS ÚMČ P7)

Vyplní vedoucí odboru: *(a dále zašle na odbor informatiky)*

Příjmení a jméno:

Odbor:

Oddělení:

Ukončení pracovního poměru ke dni:

Pokyny pro předávání elektronických dat:

Poštovní schránku:

- ☐ zrušit
- ☐ přesměrovat na 1 měsíc: komu a po té zrušit
- ☐ překopírovat zprávy: komu

Dokumenty

- ☐ smazat nenávratně
- ☐ překopírovat: komu
- ☐ archivovat a předat vedoucímu odboru

Písemnosti ve spisové službě:

- ☐ předat: komu
- ☐ ponechat na funkčním místě a přidat zastupování komu:

Písemnosti v AIP-SAFE:

- ☐ předat: komu
- ☐ ponechat na funkčním místě a přidat zastupování komu:

Kvalifikovaný zaměstnanecký certifikát ANO – NE Datum zneplatnění:

Příloha č. 3 **Vzor souhlasu se zpracováním osobních údajů**

(např.) Anketa – Bydlení na Praze 7

Zde bude text (grafika) o dané akci a formulář pro sběr údajů.

Souhlas se zpracováním osobních údajů ve smyslu GDPR[16]

Popište účel zpracování osobních údajů. Např.:

Účelem zpracování Vašich osobních údajů je získání informací o preferencích občanů v závislosti na jejich věku, povolání a bydlišti v obci v oblasti bytové politiky a následné tvorby této politiky.

Uveďte výčet osobních údajů, které se budou zpracovávat. Např.:

Budou se zpracovávat tyto osobní údaje: jméno, příjmení, adresa, email, věk, povolání, telefonní číslo.

Popište způsob, jak se bude s údaji zacházet. Např.:

Osobní údaje budu zpracovávány v elektronické formě v informačním systému na našich interních serverech. Při zpracování osobních údajů nedochází k automatizovanému rozhodování ani profilování. Osobní údaje nebudou poskytnuty žádné třetí straně. Na základě zvláštních zákonných podmínek by k těmto údajům mohly mít přístup policie a soudy, eventuálně Úřad na ochranu osobních údajů.

Uveďte dobu, po kterou se budou osobní údaje zpracovávat. Např.:

Osobní údaje budou zpracovávány po dobu trvání ankety a z důvodů zpracování dat dva měsíce po ukončení ankety.

Máte právo:

- kdykoli odvolat souhlas se zpracováním těchto svých osobních údajů a to podáním písemné žádosti ke správci (viz níže)požadovat přístup ke svým osobním údajům a poskytnutí jejich kopie
- na opravu svých osobních údajů, jsou-li nepřesné nebo neúplné
- na výmaz svých osobních údajů, jsou-li zpracovávány bez platného právního titulu
- podat stížnost u Úřadu na ochranu osobních údajů, pokud máte za to, že zpracování osobních údajů porušuje právní předpisy

Správce: Úřad MČ Praha 7, Nábřeží kpt. Jaroše 1000/7, 170 00, Praha 7, email: podatelna@praha7.cz, datová schránka: r44b2x7

Vyplňte jméno a kontakt na odpovědnou osobu. Např.:

Vyřizuje: Jan Koudelka, odbor slavností, tel: 123456789, e-mail: koudelka@praha7.cz

Pověřenec pro ochranu osobních údajů: dpo@praha7.cz

Souhlasím se zpracováním osobních údajů.

V Praze dne ..... Podpis: .....

[16] Nařízení Evropského parlamentu a rady (EU) 2016/679.