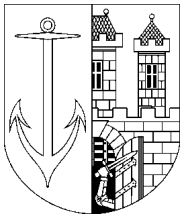
;



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

NAŘÍZENÍ

tajemníka č. xx~~2~~ ze dne ~~25.05.2018~~xx.xx.2023
s účinností od ~~25.05.2018~~01.03.2023

k ~~I~~informačnímu systému Úřadu MČ Praha 7~~y, zpracování osobních údajů a jejich ochrana~~

Schváleno usnesením Rady MČ Praha 7 č. xxxx/23-R z jednání č. xx, ze dne xx.xx.2023

OBSAH

Naformátováno: Normální, Přístupy klávesou tabulátor: není na 1,41 cm + 15,97 cm

~~10.~~1. —Účel

1. Úřad M~~ěstské části~~Č Praha 7 (dále "úřad" nebo "ÚMČ P7") vykonává agendy, jejichž součástí je zpracování[1] dat[2]. Informační systém úřadu (IS) jsou ~~digitální~~ nástroje a služby určené pro ~~toto~~ zpracování dat v elektronické podobě.

~~2.~~ Účel tohoto dokumentu je zajištění kromě jiného těchto *funkcí* úřadu:

~~2. 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).
- Zpracování dat probíhá v souladu se všemi relevantními legislativními opatřeními – zejména Zákon o ochraně osobních údajů[5] a GDPR[6].

3. Tento dokument popisuje služby a prostředky IS (viz 2. Informační systém) ~~a~~ , ~~jeho~~ pravidla používání (viz 3. Pravidla pro užívání IS), a upřesňuje pravidla stanovená ~~směrnicí~~nařízením tajemníka k nakládání s osobními údaji ~~„Nakládání s osobními údaji" pro vy~~ prostředí ~~digitální infrastruktury úřadu~~ IS (viz 4. ~~4Zpracování~~ Ochrana osobních údajů).

Naformátováno: Odsazení: Předsazení: 0,88 cm, Přístupy klávesou tabulátor: 0,39 cm, (Zarovnání vlevo) + 1,27 cm, (Zarovnání vlevo) + 1,9 cm, (Zarovnání vlevo) + není na 1,66 cm

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

~~1.~~2. Informační systém

~~1.~~ Uživatel ~~IS (dále "uživatel")~~ je osoba oprávněná~~, která může~~ používat IS ~~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://P7helpdesk~~ 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 e-mailu, telefonicky nebo osobně.

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 ~~T~~tablet je uživatelům k dispozici po schválení vedoucím odboru a tajemníkem úřadu.
4. Uživatel musí ~~N~~notebook pravidelně a na dostatečně dlouhou dobu připojovat k internetu, aby byly aktualizovány funkce a zabezpečení ~~N~~notebooku (operační systém a ostatní programové vybavení).

---

[5] Zákon 101/2000Sb., o ochraně osobních údajů
[6] Nařízení Evropského parlamentu a rady (EU) 2016/679

Naformátováno: Odsazení: Vlevo: 0,39 cm, Bez odrážek a číslování

Okomentoval(a): [KLMI1]: Jsou uživateli IS pouze zaměstnanci MČ? V návaznosti na bod 3.1 přístup IS

Okomentoval(a): [JR2R1]: Uživatelem IS je kdokoli s přístupem. Viz doplněno 3.1 – přístup schvaluje VED nebo TAJ.

Naformátováno: Odsazení: Vlevo: 1,27 cm, Bez odrážek a číslování

Změněn kód pole

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 je k dispozici s určitým hlasovým a datovým tarifem s parametry podle aktuální smlouvy s operátorem.
2. Mobilní telefon lze používat k soukromým účelům.
3. Uživatel má přístup k mobilnímu telefonu neustále pod kontrolu. Telefon je zabezpečen[7] proti přístupu jinými osobami než uživatel.
4. Bod 3. platí také pro případ, kdy je soukromý mobilní telefon využíván pro pracovní účely.

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
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.

[7] Např. heslem nebo biometrickou identifikací.

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 a certifikáty

1. Elektronické dokumenty lze opatřovat ~~kvalifikovaným~~ uznávaným elektronickým podpisem založeném~~ý~~ na kvalifikovaném certifikátu.
2. Certifikát pro~~, nezbytný pro funkci uznávaného~~ elektronick~~ého~~ podpis~~u~~ se vydává na základě žádosti.~~, dostane uživatel na základě odůvodněné žádosti příslušného vedoucího odboru. Žádost lze podat až po uplynutí zkušební doby uživatele.~~
3. Spolu s certifikátem pro elektronický podpis se vydává také komerční certifikát pro zabezpečený přístup do informačních systémů státní správy.
4. Vlastník certifikát~~ů~~ je povinen s certifikáty ~~certifikátem~~ a čipovou kartou, na které jsou uloženy, zacházet tak, že pravděpodobnost kompromitace certifikát~~ů~~ je minimální. V případě podezření na kompromitaci certifikátu (např. došlo k odcizení karta ~~certifikát byl odcizen~~), je uživatel povinen tuto situaci nahlásit IT (viz 2.1. HelpDesk), který certifikát zneplatní.
5. Při rozvázání pracovního poměru zajistí IT zneplatnění daného certifikátu na základě Výstupního listu (viz příloha Výstupní list).

Okomentoval(a): [ST3]: To si myslím, že už se neděje, a všichni to dostanou tak nějak automaticky.

Plus si myslím, že kromě kvalifikovaného je na kartě I komerční certifikát.

Okomentoval(a): [JR4R3]: Ok, doplněno "automatické" vydání podpisového certifikátu + komerční certifikát.

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 apod.) 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 / aplikace Usnesení /

Signer.

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 a platformy

1. Součástí IS jsou aplikace nebo platformy pro vedení agend. Jedná se například:
   - E-spis (elektronický systém spisové služby)
   - Ginis (finanční a ekonomické záležitosti)
   - ~~AiP Safe~~Usnesení (dokumenty pro zastupitelstvo a radu)
   - IDES (evidence nemovitostí)
   - Vita (evidence přestupků, stavební úřad)
   - Datacentrum Personalistika (personální a mzdový SW~~swevidence~~)
   - ~~Datacentrum~~ Docházka (evidence docházky)
   - Microsoft 365 (dříve Office 365)

~~12.~~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 s výjimkou mobilního telefonu) 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[8] 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

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

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 e-mailů), 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.
17. Je zakázáno používat jakékoli cloudové platformy pod soukromým účtem pro ukládání dat úřadu.
18. Uživatel, který opouští pracoviště jako poslední, je povinen daný prostor zabezpečit proti přístupu neoprávněných osob.
19. Uživatel odpovídá za to, že na pracovišti nebudou ponechána volně přístupná data (listinná nebo elektronická) služebního charakteru ani data nebo software nesložebního charakteru.

3.1. Přístup k IS

1. Osoba se stane uživatelem IS přidělením přístupu do IS.
2. Rozsah přístupu nastavuje IT na základě žádosti vystavené schválené vedoucím odboru nebo tajemníkem a zaslané IT (viz 2.1. HelpDesk).
3. U nového zaměstnance je součástí žádosti "Vstupní list" (viz. pPříloha 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[9] 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 Vvýstupní list (viz Ppříloha č. 2). IT zodpovídá za to, že všechny přístupy daného zaměstnance budou zneplatněny nejpozději k datu uvedenému ve Vvýstupním

Naformátováno: Bez odrážek a číslování

[9] Minimální délka 8 znaků, alespoň jedno malé písmeno, alespoň jedno velké písmeno, alespoň jedna

listu.

~~10.~~8. Externí uživatel[10] 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. Odbor informačních technologií (IT)~~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[11].

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.~~

~~číslice, alespoň jeden speciální znak.~~

[10] Např. dodavatel části IS.

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

2. [illegible]

13.4. ZpracováníOchrana osobních údajů

1. Obecná pPravidla pro zpracování osobních údajů v rámci úřadu stanovuje nařízení tajemníka k „Nnakládání s osobními údaji“.

1.2. Uživatelé dbají zvýšené opatrnostiÚřad MČ Praha 7 je ve smyslu GDPR[12] správce[13] a zpracovatel[14] 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[15] nebo soustava operací systematicky prováděná s osobními údaji. , když dochází ke komunikaci osobních údajů z IS k externím příjemcům.

3. Osobní údaje odesílané mimo úřad (např. e-mailem, nebo jiným kanálem) 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. uživatel zabalí do ZIP souboru zabezpečeného heslem. Heslo odešle příjemci jiným komunikačním kanálem – např. SMSkou.

4. Přístup (odkaz) k osobním údajům uloženým v systému Microsoft 365 (dříve Office 365) příjemci mimo úřad uživatel zabezpečí pomocí hesla. Heslo sdělí příjemci jiným kanálem, než kterým příjemce obdržel odkaz. Odkaz se většinou posílá e-mailem, heslo pak SMSkou.

2.5. Platí zákaz zpracování osobních údajů jakýmkoli nástrojem nebo (cloudovou) službou pod soukromým nebo anonymním účtem.

3. Ke zpracování OÚ může docházet na základě souhlasu SÚ nebo zákonného důvodu.

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.

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

„ otisk úředního razítka“

Příloha č. 1 – Vstupní list nového zaměstnance

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~~Aplikace Usnesení ~~+ 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 Úřadu MČ Praha 7

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~~Aplikaci Usnesení:
- ☐ 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**~~

Okomentoval(a): [KLMI5]: Příloha č. 3 by neměla být již součástí nařízení, jelikož s ním nijak nesouvisí

Okomentoval(a): [JR6R5]: odstraněno