Zpráva nezávislého auditora

o ověření shody s požadavky GDPR

Statutární město Chomutov

Datum vyhotovení: 17.květen 2018

OBSAH

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

1. SEZNAM ZKRATEK

Zkratka	Vysvětlení zkratky
DPIA	Data Protection Impact Assessment (posouzení vlivu na ochranu osobních údajů)
Město	Statutární město Chomutov/ Magistrát města Chomutov
EU	Evropská unie
GDPR	General Data Protection Regulation (obecné nařízení o ochraně osobních údajů)
IS	Informační systém
TQM	Total Quality Management (komplexní řízení kvality)
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů
ZSS	zákon č. 108/2006 Sb., o sociálních službách

Upozornění zpracovatele tohoto formuláře:

Auditoři BDO Advisory s. r. o. budou zpracovávat zprávu o stavu připravenosti Vašeho Města na základě informací poskytnutých Vaším Městem ve formě tohoto vyplněného dotazníku, případně písemných podkladů (směrnice, nařízení, rozhodnutí apod.) vyžádaných tímto dotazníkem, veřejných informací a případné návštěvy a rozhovoru se zástupci Vašeho Města.

V případě, že bude Dotazník vyplněn nedostatečně, tj. budou poskytnuty informace neúplné, nepřesné či nebudou poskytnuty vůbec, pokusí se následně auditoři o dodatečné získání či doplnění informací (telefonicky či mailem). V případě, že ani dodatečné informace neposkytnou relevantní odpověď na danou otázku, využijí auditoři tzv. „princip opatrnosti“ a přiřadí dané problematice o stupeň vyšší riziko.“

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

2. PŘEDMĚT AUDITU

Na základě dohody bylo uskutečněno nezávislé ověření shody současného nastavení a fungování procesů a bezpečnostních opatření ve **Statutárním městě Chomutov** s požadavky stanovenými GDPR.

Byly prověřeny procesy zpracování osobních údajů z následujících hledisek:

- dodržování zásad zpracování osobních údajů,
- vedení dokumentace systému řízení osobních údajů,
- nastavení a fungování organizačních opatření,
- řízení lidských zdrojů z pohledu bezpečnosti osobních údajů,
- nastavení a fungování technických opatření.

Podrobná metodika realizace auditu tvoří Přílohu č. 1 tohoto dokumentu.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

3. ZÁKLADNÍ CHARAKTERISTIKA ORGANIZACE

Město Chomutov je statutárním městem v Ústeckém kraji. Je 22. největším městem v České republice a žije v něm přibližně 49 tisíc obyvatel

Magistrát města je členěn do těchto odborů:

- Úsek kancelář tajemníka
- Odbor majetku města
- Odbor školství
- Odbor informačních technologií
- Odbor rozvoje a investic
- Odbor dopravních a správních činností
- Odbor ekonomiky
- Odbor životního prostředí
- Odbor stavební úřad
- Odbor interní audit
- Odbor sociálních věcí
- Odbor vnějších vztahů

Město Chomutov je spravováno zastupitelstvem, které rozhoduje o majetkoprávních úkonech obce a dalších záležitostech dle zákona č. 128/2000 Sb. o obcích a jeho novel. Rada je výkonným orgánem Města a zodpovídá se právě zastupitelstvu obce. Ve vedení města pak stojí primátor a jeho náměstci.

Dále je v rámci samostatného útvaru zajišťována mzdová a personální agenda pro pracovníky magistrátu.

Město je zřizovatelem mateřské, umělecké, základních škol, příspěvkových organizací a má zároveň i organizační složky. Všechny tyto subjekty jsou uvedeny v Příloze č. 3.

Pro zajištění připravenosti souladu všech agend Města a jeho organizací byl vytvořen interní Projektový tým GDPR a již v roce 2017 byla provedena první analýza stavu zpracování a ochrany osobních údajů, která byla zpracována po jednotlivých odborech a organizacích.

Výstupy z této analýzy byly poskytnuty společnosti BDO Advisory s.r.o. Vzor takového výstupu je uveden v Příloze č. 4

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

3.1 Identifikované oblasti zpracování osobních údajů

Zpracování osobních údajů se v identifikovaných oblastech řídí následujícími předpisy (výčet legislativy není kompletní z důvodu jeho rozsáhlosti):

- zákon č. 128/2000 Sb., o obcích,
- zákon č. 129/2000 Sb., o krajích,
- zákon č. 101/2000 Sb., o ochraně osobních údajů,
- nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) – účinnost od 25. května 2018,
- zákon č. 262/2006 Sb., zákoník práce,
- zákon č. 312/2002 Sb., o úřednících územních samosprávných celků,
- zákon č. 435/2004 Sb., zákon o zaměstnanosti,
- zákon č. 563/1991 Sb., zákon o účetnictví,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě,
- zákon č. 222/1999 Sb. o zajišťování obrany ČR,
- zákon č. 237/2000 Sb., o požární ochraně,
- zákon č. 238/2000 Sb., o Hasičském záchranném sboru ČR,
- zákon č. 239/2000 Sb., o Integrovaném záchranném systému,
- zákon č. 240/2000 Sb., o krizovém řízení,
- zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy,
- zákon č. 585/2004 Sb., branný zákon,
- zákon č. 183/2006 Sb., o územním plánování a stavebním řádu,
- zákon č. 134/2016 Sb., o zadávání veřejných zakázek,
- zákon č. 301/2000 Sb., o matrikách, jménu a příjmení,
- zákon č. 133/2000 Sb. o evidenci obyvatel a rodných číslech,
- zákon č. 500/2004 Sb., správní řád,
- zákon č. 89/2012 Sb., občanský zákoník,
- zákon č. 337/1992 Sb., o správě daní a poplatků,
- zákon č. 247/2000 Sb., o získávání odborné způsobilosti k řízení vozidel,
- zákon č. 361/2000 Sb., o provozu na pozemních komunikacích,

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

- zákon č. 269/2007 Sb., o informačních systémech veřejné správy,
- zákon č. 21/2006 Sb., o ověřování shody opisů nebo kopie s listinou a ověřování pravosti,
- zákon č. 328/1999 Sb., o občanských průkazech.

3.2 Identifikované oblasti správy a zpracování osobních údajů

Audit zjistil, že Město zpracovává osobní údaje v rámci následujících činností (procesů):

- evidence obyvatel,
- zajišťování voleb ve Městě,
- zabezpečování ochrany veřejného pořádku, Městské policie,
- při jednáních vedení obce/zastupitelů a v návazných zápisech či usneseních,
- sjednávání a uzavírání smluvních ujednání,
- správa a výběr správních/místních poplatků,
- zajišťování kulturního života obce včetně vítání občánků, evidence jubileí apod.,
- vedení kroniky,
- zdokumentování, informování o životě ve Městě, a to i za pomoci fotografických a jiných médií.
- zajišťování vidimace a legalizace,
- poskytování sociálních služeb přes vlastní příspěvkovou organizaci,
- zajištění personálních činností, mezd a vedení účetnictví (týká se i všech složek a organizací Města),
- zřizovatel škol a školských organizací
- zřizovatel příspěvkových organizací,
- zřizovatel organizačních složek.

V souvislosti se zpracováním osobních údajů vystupuje Město jako správce osobních údajů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

4. OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR)

Evropský parlament schválil 14. dubna 2016 Obecné nařízení o ochraně osobních údajů („GDPR“). Účinnost tohoto nařízení nastává 25. května 2018. Pro všechny subjekty, které zpracovávají osobní údaje občanů Evropské unie („EU“), znamená toto opatření upřesnění či vznik nových povinností v souvislosti se zvýšením ochrany a práv občanů Evropské unie.

GDPR je vydáno formou přímo účinného nařízení, které není nutno transponovat do právních řádů členských států. V České republice toto nařízení nahradí současnou právní úpravu ochrany osobních údajů. Níže jsou uvedeny změny a jejich dopady, které GDPR vyvolává:

- zpřísnění podmínek pro evidenci a zpracování osobních údajů, a to jak ve zcela nebo částečně automatizovaném, tak i v neautomatizovaném zpracování,
- přísnější požadavky na podobu souhlasu se zpracováním osobních údajů od subjektu údajů a výslovně zakotvené právo souhlas odvolat,
- nová práva subjektů údajů jako např. právo na přenositelnost údajů, nebo významné posílení stávajících práv jako např. práva být zapomenut,
- širší informační povinnost – správce je povinen subjekty údajů dostatečně a srozumitelně informovat, např. o účelu a právním základu zpracování osobních údajů, o jejich právech atd.,
- nové požadavky na obsah smlouvy uzavřené mezi správcem a zpracovatelem,
- přísnější požadavky na zabezpečení osobních údajů – i když je nařízení založeno na principu technologické neutrality, zmiňuje možná technická opatření sloužící k ochraně integrity, důvěrnosti a dostupnosti dat,
- povinnost zohledňovat požadavky GDPR již při zavádění nebo úpravě stávajících procesů GDPR (zásada Privacy by design) a aplikace nejpřísnějšího režimu ochrany osobních dat (zásada Privacy by default),
- přísnější nároky na dokumentaci zpracování osobních údajů,
- v případě vysokého rizika pro práva a svobody subjektů údajů musí být zpracováno posouzení vlivu na ochranu osobních údajů („DPIA“),
- požadavek na reportování porušení zásad ochrany dat jak příslušnému orgánu, tak i subjektu údajů.
- ve vybraných případech povinnost jmenovat Pověřence pro ochranu osobních údajů (DPO).
- nařízení upravuje výši sankcí pro organizace při nedodržení podmínek GDPR.

Porušení výše uvedených povinností může vyústit v pokutu ve výši až 20 mil. EUR. Popsané změny musí správci a zpracovatelé osobních údajů zahrnout do svých systémů řízení,

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

firemních (organizačních) procesů včetně úpravy příslušných dokumentací, či provedení úprav dodávaných produktů.

4.1 Oblasti působení z pohledu osobních údajů

4.1.1 Zdroje osobních údajů

Město shromažďuje a zpracovává osobní údaje fyzických osob, které mají zájem o jeho služby či spadají pod jeho působnost. Údaje jsou získávány od státní správy, podřízených organizací či přímo od subjektů osobních údajů. Osobní údaje jsou získávány jak v elektronické formě, například přístupem do různých portálových aplikací, v listinné podobě (od subjektů údajů/občanů či třetích stran), i ústně v rámci komunikace s občany. Další osobní údaje jsou získávány v průběhu realizace potřebných kroků při řešení příslušné záležitosti/agendy.

4.1.2 Umístění osobních údajů

Osobní údaje jsou uchovávány buď v listinné podobě na jednotlivých odborech úřadu, nebo v elektronické podobě v příslušných aplikacích Města a státní správy (***IS Gordic, IS Vita sofware a další)***. Obvykle jsou osobní údaje zpracovávány také za pomoci běžného kancelářského SW. Osobní údaje mohou být také obsahem emailové komunikace. Fyzicky jsou elektronická data umístěna v počítačové síti Města.

4.2 Zajištění personálních činností, mezd a účetnictví

4.2.1 Zdroje osobních údajů

Údaje jsou získávány přímo od dotčených zaměstnanců při nástupu do pracovního/služebního poměru a to písemně (např. občanské průkazy – kontrola a opis dat, potvrzení o zaměstnání od předchozího zaměstnavatele, pracovní posudky, dotazníky, žádosti, životopisy, žádosti o přijetí, zdravotní prohlídky, doklady o dosaženém vzdělání a praxi, výpisy z rejstříku trestů, písemná potvrzení o absolvování školení, osvědčení o odborné způsobilosti apod.), nebo ústně (nahlašování změn, doplnění údajů při rozšíření požadavků dle zastávané pracovní pozice).

4.2.2 Umístění osobních údajů

Osobní údaje zaměstnanců v papírové podobě jsou shromažďovány v osobním spisu zaměstnanců, který vede personalistka úřadu, dále je zpracovává také mzdová účetní. Osobní údaje v elektronické podobě jsou vedeny ve mzdovém software a jsou také součástí kancelářského office včetně emailové komunikace. Přístup k osobním údajům zaměstnanců vedeným elektronicky je možný pouze pro oprávněné osoby za pomoci přístupového hesla (přístup do příslušných IS).

4.2.3 Smlouvy a dohody

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Součástí pracovních smluv, dohod o provedení práce a srovnatelných dokumentů by mělo být vyjma ustanovení, že byl zaměstnanec seznámen se svými povinnostmi při výkonu své práce a plnění dalších úkolů stanovených zaměstnavatelem vždy také ustanovení o povinnosti dodržovat mlčenlivost o všech skutečnostech, které se při výkonu své práce dozví (občané, kolegové a dalších) a to jak v době trvání pracovního poměru (výkonu práce v rámci dohody o práci konané mimo pracovní poměr), tak i po jeho skončení.

4.2.4 Výběrové řízení

Součástí výběru budoucích zaměstnanců je hodnocení informací obsažených v životopisech, které Město obdrželo od uchazečů o zaměstnání. Po skončení výběrových řízení jsou životopisy neúspěšných kandidátů uloženy spolu s dokumentací VŘ. Ve zveřejněných nabídkách příslušných pracovních pozic se po uchazečích nepožaduje souhlas se zpracováním osobních údajů, a to ani po skončení výběrové řízení. Tento přístup je v souladu s GDPR (jedná se o jednání za účelem uzavření smlouvy). V případě možného obdržení nevyžádaných nabídek práce, lze zvolit jeden ze dvou možných přístupů, a to buď tyto skartovat, nebo si vyžádat od žadatele o práci souhlas se zpracováním poskytnutých údajů.

4.2.5 Další zpracovávané osobní údaje

Kromě standardních osobních údajů, které jsou nutné pro zajištění personálních činností, včetně zpracování mezd a povinných odvodů, Město nezpracovává žádné jiné osobní údaje, a to ani obrazové záznamy zaměstnanců (fotografie) zachycující zaměstnance při aktivitách souvisejících s poskytováním služeb obyvatelům. Za výjimku lze považovat fotografie statutárních a volených zástupců (Rada + Zastupitelstvo) zveřejněných na webu Města, kde tito zástupci vystupují jako veřejné osoby, tedy není třeba ošetřit prostřednictvím „Souhlasu“. V případě, že by se fotografie zaměstnanců/úředníků úřadu měla objevit v místních novinách, na úřední desce, webu města apod., v takové formě, kdy lze pracovníka jednoznačně identifikovat (upraveno mimo GDPR i v již od roku 2014 účinném Občanském zákoníku, § 84), je nezbytné získat od zaměstnance souhlas s fotografováním.

4.2.6 Zpracování po ukončení pracovněprávního vztahu

Po ukončení pracovněprávního vztahu jsou všechny písemnosti tvořící osobní spis zaměstnance dále uchovávány, aniž by byly vybrány ty, které lze ihned zlikvidovat. Otázkou je, zda tento systém není v rozporu se spisovým a skartačním řádem a zda by neměly být vybrány ty, které lze ihned skartovat. Protože pokud nehovoří spisový a skartační řád jinak, tak dle GDPR by měly být nepotřebné dokumenty zničeny v souladu s čl. 17 GDPR.

4.2.7 Povaha zpracovávaných osobních údajů

Osobní údaje, které jsou zpracovávány v souvislosti se zajištěním personální činnosti, mezd a účetnictví, obvykle nespadají do zvláštní kategorie osobních údajů (nejsou citlivými údaji). Za jedinou výjimku lze považovat informace o zdravotním stavu zaměstnanců (vstupní a

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

následné periodické zdravotní prohlídky). Ze zprávy o provedené zdravotní prohlídce, kterou získává zaměstnavatel od zaměstnanců, lze dovodit také informace o zdravotním stavu zaměstnance (je-li uvedeno určité omezení, či dokonce dg). Zprávy jsou součástí osobní složky zaměstnance.

4.3 Zabezpečení zpracovávaných údajů

Data vedená v elektronické podobě jsou poměrně dostatečně zabezpečena, přístup do PC je vždy chráněn heslem. Díky tomu, že v současnosti už téměř nikdo z běžných uživatelů není veden jako administrátor, nemá přístup k diskům a tedy i osobním datům, která může zneužít. Notebooky většinou neopouští Město (pouze přesun mezi budovami Města, organizacemi či patry budov), „chytré“ mobilní telefony, které má k dispozici několik zaměstnanců jsou v některých případech používány k přístupu do e-mailů., nikde není nainstalován již neaktualizovaný kancelářský SW (např. XP). Zálohování dat probíhá denně a dle plánu záloh.

Daná problematika (ochrana osobních údajů, práce s IT) by také měla být ošetřena ve směrnici upravující jednak IT a dále také ve směrnici upravující ochranu osobních dat v organizaci.

Dokumenty v listinné podobě nejsou vždy uzamykány v uzamykatelných skříních či registraturách v kancelářích, mohou být i na stolech přístupných návštěvníkům Města. Problematika rezervních klíčů a čipových karet je řešena individuálně na jednotlivých budovách a provozech Města.

Je potřeba působit především v rámci zvyšování povědomí zaměstnanců o ochraně osobních dat, ideálně formou krátkých školení, v podstatě mohou být tato školení zařazena jako součást běžných porad, při kterých se setkávají všichni zaměstnanci.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

5. MANAŽERSKÉ SHRNUTÍ ZJIŠTĚNÍ AUDITU

Zjištění uvedená v této zprávě jsou kategorizována z hlediska jejich významu dle níže uvedené tabulky.

Významnost zjištění	Symbol	Popis
Vysoké riziko		Zjištění vysoké významností, jsou zanedbány klíčové požadavky Nařízení GDPR. Existuje vysoké riziko sankcí.
Střední riziko		Zjištění středné významnosti, některé požadavky Nařízení GDPR nejsou uplatňovány.
Nízké riziko		Zjištění nízké významnosti, některé požadavky nařízení GDPR nejsou uplatňovány, avšak jedná se o administrativní či jiné nezávažné nedostatky.

Souhrn klíčových zjištění auditu

V tabulce níže jsou shrnuta klíčová zjištění auditu (střední, vysoké riziko). Detailní popis všech zjištění je uveden v kapitolách 6. a 7. této zprávy.

ID	Významnost zjištění	Název zjištění
1.		**Chybějící role/odpovědnost za ochranu osobních údajů**
2.		**Chybějící směrnice na ochranu osobních údajů a nedostatečná směrnice pro oblast práce s IT technikou v celém rozsahu**
3.		**Chybějící/Nedostatečná matice rolí a přístupů k OÚ a klíčového hospodářství**
4.		**Chybějící/Nedostatečná evidence uchovávaných/zpracovávaných osobních údajů včetně umístění**
5.		**Neplnění/Nedostatečné plnění informační povinnosti o zpracování osobních údajů**
6.		**Souhlas se zpracováním OÚ - více nálezů**

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

7.		**Zpracování OÚ a zvláštní kategorie údajů, které nejsou nezbytně nutné - zaměstnanci/uchazeči o zaměstnání**
8.		**Neoprávněně pořizování fotokopií občanských průkazů**
9.		**Neprovádění aktualizace spisů a Nestanovení/nedodržování skartační lhůty**
10.		**Nedostatečně upravený vztah se zpracovatelem osobních údajů**
11.		**Nedostatečná fyzická bezpečnost - listinné a elektronické dokumenty**
12.		**Bezpečnost IT - více nálezů**
13.		**Nesledování aktuálních bezpečnostních hrozeb a neprovádění testů zranitelnosti ICT**
14.		**Komunikační kanály - nezabezpečená e-mailová komunikace**
15.		**Neprovádění analýzy rizik pro práva a svobody subjektů údajů a krizového plánu**
16.		**Nedostatečná vnitřní úprava povinností mlčenlivosti**
17.		**Školení - Neprovádění systematického zvyšování povědomí o ochraně osobních údajů a o jejich zabezpečení**
18.		**Povinnost jmenovat pověřence pro ochranu osobních údajů**

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

6. PODROBNÝ POPIS ZJIŠTĚNÍ DOPORUČENÍ AUDITU

V této kapitole jsou podrobně popsána veškerá zjištění realizovaného auditu. U každého zjištění je identifikována jeho závažnost a návrh optimalizačních opatření vedoucí k odstranění negativních zjištění. Auditor konstatuje, že v této kapitole jsou popsána výhradně negativní zjištění. Pozitivní zjištění (ta zjištění, která poukazují na správnost nastavení systému správy a zpracování osobních údajů), nejsou předmětem tohoto dokumentu.

Auditor dále konstatuje, že jednotlivé významnosti zjištění byly uděleny v kombinaci vlastního nálezu příslušného nedostatku a stupně závažnosti/významnosti, který deklaroval do současnosti dozorový orgán nad GDPR, tj. Úřad na ochranu osobních údajů.

Proto i zjištění, která nedosahují maximálního rizika či významnosti, mohou být označena jako kritická, právě s ohledem na kritický pohled ÚOOÚ na tuto specifickou problematiku.

Zjištění pro jednotlivé odbory Města jsou uvedena v kapitole 7. této zprávy

6.1 Zjištění a doporučení:

Legislativní rámec:

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku. Podle odst. 2 daného ustanovení se při posuzování vhodné úrovně zabezpečení zohlední zejm. rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

1.		**Chybějící role/odpovědnost za ochranu osobních údajů**
Zjištění:		V organizačním řádu / struktuře není definována pozice/role, která má ve své kompetenci odpovědnost za procesy řešící ochranu osobních údajů v prostředí společnosti.
Doporučení:		Definovat v organizačním řádu či v organizační struktuře roli, v jejíž pracovní náplni bude definovat, řídit i kontrolovat činnosti s dopadem na ochranu osobních údajů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	Obsazení této role není splněním povinnosti mít stanoveného Pověřence na ochranu osobních údajů – DPO dle GDPR.

6.2 Směrnice na ochranu osobních údajů a práce s IT

Legislativní rámec:

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku. Podle odst. 2 daného ustanovení se při posuzování vhodné úrovně zabezpečení zohlední zejm. rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Obdobná pravidla plynou z aktuálně účinného § 13 ZOOÚ, přičemž podle odst. 2 citovaného ustanovení je správce povinen přijatá a provedená opatření zdokumentovat.

Podle části 5.2 mezinárodně uznávaného standardu ISO/IEC 27001 vrcholové vedení organizace zavede zdokumentovanou politiku (pravidla) bezpečnosti informací. Součástí těchto pravidel by měla být také pravidla upravující rozsah přístupových oprávnění jednotlivých zaměstnanců k informacím a k zařízením, kde jsou informace, včetně osobních údajů, uloženy a zpracovávány (bod A.9 ISO/IEC 27001). Vrcholové vedení by tak mělo stanovit např. jednotná pravidla pro zajištění kvality hesel a zavést technická opatření vynucující automatizované uplatňování stanovených pravidel (např. příslušná aplikace bude v pravidelných intervalech vyžadovat změnu hesla, nové heslo musí mít definovaný počet a strukturu znaků).

2.		**Chybějící směrnice na ochranu osobních údajů a nedostatečná směrnice pro oblast práce s IT technikou v celém rozsahu**
Zjištění:		Město nemá vytvořenou směrnice na ochranu osobních údajů všech subjektů osobních údajů (zaměstnanci, popř. ostatní osoby a další), obsahující všechny předepsané náležitosti. Pokud je ochrana osobních údajů zmíněna v ostatní interní dokumentaci Města formou odkazů či citací, pak je víceméně v souladu se stávající platnou legislativou, tj. zákonem 101/2000 Sb. O ochraně osobních údajů a neodpovídá tak novému nařízení GDPR.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 1:	Zpracovat dokument/směrnici na ochranu osobních údajů všech subjektů. Může být zpracována dle vzoru přiloženého obsahu. <u>Směrnice o ochraně osobních údajů – obsah:</u> 1. **Úvodní ustanovení** (účel a působnost, vymezení pojmů, zkratky) 2. **Zásady zpracování osobních údajů** (zásady, zákonnost zpracování, souhlas subjektu údajů, odvolání souhlasu, oprávněný zájem správce, zvláštní kategorie osobních údajů - citlivé údaje) 3. **Práva subjektů údajů** (definování práv subjektů údajů, postupy správce při výkonu práv subjektů údajů, plnění informační povinnosti vůči subjektu údajů) 4. **Povinnosti správce při zpracování osobních údajů** (obecné povinnosti, odpovědnost správce za zpracování, zpracování osobních údajů zpracovatelem, odpovědnost zpracovatele, odpovědnost a povinnosti pověřených osob při zpracování osobních údajů, spolupráce s dozorovým úřadem, posouzení vlivu na ochranu osobních údajů) 5. **Záznamy o činnostech zpracování** 6. **Zpracování osobních údajů v rámci organizace** (členění dle typů prováděných operací) 7. **Zabezpečení osobních údajů** (organizační a technická opatření, ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu, posouzení vlivu na ochranu osobních údajů) 8. **Předávání osobních údajů** (předávání v rámci ČR, předávání v rámci EU, předávání do třetích zemí) 9. **Kontrola ochrany osobních údajů** (kontrola v rámci organizace, kontrolo prováděná dozorovým úřadem) 10. **Související dokumenty** 11. **Závěrečná ustanovení**
Doporučení 2:	Aktualizovat stávající směrnici upravující oblast IT na magistrátu tak, aby obsahovala všechny níže uvedené oblasti: ▶ Bezpečnostní zásady - vyhlášení zásad zabezpečování informací, například lze použít uváděné bezpečnostní desatero v rámci zvyšování bezpečnostního povědomí zaměstnanců;

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	▶ Organizování bezpečnosti – do organizačního řádu uvést závazek vedení Města na ochranu osobních údajů; ▶ Zabezpečení přístupu třetích stran – uvést, že přístup k osobním údajům mají pouze zaměstnanci a třetí strany/zpracovatelé jen na základě smluvního ošetření; ▶ Personální bezpečnost; ▶ Reakce na incidenty – v organizačním řádu uvést, že komunikovat s UOOU a řešit bezpečnostní incidenty smí pouze vedení organizace či jím pověřená osoba; ▶ Řízení fyzického přístupu - popis bezpečnostních pravidel pro práci s osobními údaji včetně použití nástrojů na ochranu dat, například antivir; ▶ Bezpečná likvidace osobních údajů – zde dát povinnost vše skartovat, a to včetně fyzické likvidace nepoužívaných paměťových médií (flash disky); ▶ Provozní postupy a povinnosti – zde použít rozdělení povinností mezi jednotlivé typické pracovní pozice; ▶ Havarijní plánování – mít například připravené plány pro případ, kdy složky/SW s osobními údaji nebudou k dispozici, pro případ kyber útoku apod.; Průběžně a nadále proškolovat zaměstnance v oblasti práce s IT.

6.3 Matice rolí a přístupů, klíčové hospodářství

Legislativní rámec:

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku.

Podle odst. 2 daného ustanovení se při posuzování vhodné úrovně zabezpečení zohlední zejm. rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Z výše uvedeného vyplývá povinnost systematického zdokumentování řízení přístupů, ať už fyzických (vč. klíčového hospodářství) nebo do všech používaných IS.

Podle čl. 24 odst. 1 GDPR je správce povinen zavést vhodná technická a organizační opatření, aby zajistil, že zpracování osobních údajů bude v souladu s požadavky GDPR. Jedním z předpokladů dosažení souladu s povinnostmi stanovenými GDPR je získání a udržování zdrojů

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

nutných pro řádné fungování systému bezpečnosti informací (bod 7.1 ISO/IEC 27001). Mezi uvedené zdroje patří také dostatečné kvalifikovaný personál vykonávající činnosti, které ovlivňují úroveň bezpečnosti informací (např. IT pracovníci a IT specialisté). Vrcholové vedení by mělo mít náhradní řešení pro případ výpadku těchto klíčových zaměstnanců.

Zjištění a doporučení:

3.	**Chybějící matice rolí a přístupů k OÚ a klíčového hospodářství**
Zjištění:	V organizačním řádu ani jinde není definována pozice/role: ▶ Zodpovědné za procesy řešící ochranu osobních údajů v prostředí organizace a jejího zástupce; a dále není dostatečně zdokumentováno dle pozic/rolí: ▶ Kdo a jakým způsobem má právo s osobními údaji jednotlivých typů subjektů pracovat; ▶ Přístupová práva všech uživatelů do všech užívaných IS; ▶ Klíčové hospodářství - fyzické vstupy do jednotlivých místností, budov, spisovny/archivu, uzamykatelných skříní a kartoték apod., ve kterých jsou uchovávány dokumenty obsahující dokumenty s OÚ.
Doporučení 1:	Na základě definovaných typů pracovních pozic/rolí, vypracovat matici rolí a odpovědností, která bude jasně definovat, kdo a jakým způsobem má právo s osobními údaji jednotlivých typů subjektů pracovat.
Doporučení 2:	Následně ve vypracované matici určit pozici/roli: ▶ zodpovědnou za ochranu osobních údajů, vč. jejího zástupce; ▶ IT specialisty, vč. jeho zástupce. V rámci procesů pro IT řízení stanovit jasná pravidla a postupy pro řešení případné nedostupnosti pracovníků zajišťujících podporu kritických služeb.
Doporučení 3:	Vypracovat matici rolí a odpovědností, která bude jasně definovat přístupy všech uživatelů k listinné i elektronické podobě zpracovávaných OÚ.
Doporučení 4:	Obdobným způsobem vypracovat matici pro klíčové hospodářství, vč. osoby, která má ve své kompetenci odpovědnost za vedení evidence o počtu a pohybu klíčů. Toto platí zejména u klíčů s generálním přístupem.

6.4 Evidence uchovávaných/zpracovávaných osobních údajů včetně umístění

Legislativní rámec:

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku.

Podle odst. 2 tohoto ustanovení, se při posuzování vhodné úrovně zabezpečení zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Aby bylo možné účinně dodržet ustanovení tohoto článku, vzniká povinnost vypracovat evidenci uchovávaných či zpracovávaných osobních údajů.

Zjištění a doporučení:

<table>
<tr><td>4.  </td><td>Chybějící evidence uchovávaných/zpracovávaných osobních údajů včetně umístění</td></tr>
<tr><td>Zjištění:</td><td>Není vypracována evidence/seznam všech uchovávaných a zpracovávaných osobních údajů.</td></tr>
<tr><td>Doporučení 1:</td><td>Vytvořit evidenci všech osobních údajů shromažďovaných a zpracovávaných na magistrátu tak, aby byly shromažďovány pouze údaje skutečně nezbytné pro zajištění příslušných činností, tj. u každého kategorie OÚ musí být stanoven uplatnitelný právní titul pro zpracování.

V evidenci osobních údajů musí být vypsané i typové osobní údaje, např. včetně žadatelů, stážistů, dobrovolníků či dárců, OÚ kontaktních osob či rodinných příslušníků, uchazečů o zaměstnání apod. tak, aby byla evidence úplná.

▶ Příklad tabulkové formy, kterou je třeba přizpůsobit potřebám organizace:

<table>
<tr><th>Kategorie osobního údaje</th><th>Povaha osobního údaje</th><th>Účel zpracování</th><th>Právní důvod zpracování</th><th>Místo zpracování</th><th>Osoby/útvar provádějící zpracování</th><th>Způsob získávání</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Doporučení 2:</td><td>Uložení listinné i elektronické dokumentace s osobními údaji musí být stanoveno tak, aby se k dokumentaci dostaly pouze oprávněné osoby, tzn., že musí respektovat rozdělení pravomocí a odpovědností jednotlivých rolí zaměstnanců.
Minimálním požadavkem je fyzické uzamčení místnosti s dokumentací s tím, že klíč mají k dispozici jen oprávněné osoby. Toto platí zejména u klíčů s generálním přístupem.</td></tr>
</table>

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	U místností, kam má přístup větší množství pracovníků, kteří nemají mít přístup k údajům, pak dokumenty s osobními údaji musí být v uzamykatelných skříních.

6.5 Informační povinnost o zpracování osobních údajů

Legislativní rámec:

Čl. 12 odst. 1 stanoví povinnost správce poskytnout SÚ stručným, jasným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, veškeré informace uvedené v čl. 13 a čl. 14 GDPR (v okamžiku získání osobních údajů od SÚ nebo od jiného zdroje) a uvedl veškerá sdělení podle čl. 15 až 22 a 34. Jedná se zejména o identifikační a kontaktní údaje správce, účely zpracování, pro které jsou údaje určeny, právní základ zpracování a informace o případných příjemcích osobních údajů. Správce dále poskytuje zejm. informace o době, po kterou budou osobní údaje uloženy a informace o právech subjektu údajů zaručených GDPR a porušení zabezpečení.

Zjištění a doporučení:

5/1	**Neplnění/ plnění informační povinnosti o zpracování osobních údajů**
Zjištění:	Město v okamžiku získání osobních údajů, které nevyžadují souhlas se zpracováním od subjektů údajů, neplní svou informační povinnost vůči uchazečům o zaměstnání, zaměstnancům, žadatelům o poskytnutí služby, klientům a dalším subjektům údajů.
Doporučení 1:	Zpracovat informační memorandum, odkud subjekt údajů získá informace o správci, DPO, účelu a způsobu zpracování OÚ, základních/obecných principech ochrany OÚ, životním cyklu OÚ apod., jako samostatný dokument. Jde o to, aby informační memorandum obsahovalo potřebné náležitosti (zásady zpracování, práva subjektů, apod.) a bylo řádně naformulováno. Informační memorandum je třeba zveřejnit s účinností od 25.5.2018 např. na internetových stránkách, vyvěšením na nástěnku ve veřejném prostoru organizace, také je možné ho v budoucnu přikládat ke smlouvám apod.
Doporučení 2:	Obdobnou informaci musí mít k dispozici všechny kategorie subjektů (zaměstnanci, žadatelé, návštěvníci, klienti, stážisté, dárci, návštěvníci webových stránek při registraci a další).

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 3:	U uchazečů o zaměstnání a žadatelů o poskytnutí služby lze informační memorandum uplatňovat pouze do doby vydání rozhodnutí o přijetí či odmítnutí. Poté je nutné OÚ buď: ▶ vrátit/zlikvidovat/vymazat a informovat subjekt údajů, že jeho OÚ již nejsou dále zpracovávány nebo; ▶ si vyžádat souhlas s dalším zpracováním nebo; ▶ v případě, že byl uzavřen pracovněprávní či obchodní či jiný vztah zakládající právní nárok na zpracování, splnit vůči subjektu údajů novou informační povinnost.

6.6 Souhlas se zpracováním osobních údajů

Legislativní rámec:

GDPR v čl. 6 odst. 1 stanoví, že zpracování je zákonné, pokud je naplněn jeden ze šesti možných právních titulů zpracování uvedených v tomto odstavci. Současně písm. a) tohoto odstavce definuje jako legitimní právní titul souhlas subjektu údajů se zpracováním OÚ pro jeden či více konkrétních účelů.

Souhlas musí být poskytnut způsobem dle čl. 12 odst. 1 a dále musí obsahovat informace uvedené v čl. 13 a čl. 14 GDPR (v okamžiku získání osobních údajů od SÚ nebo od jiného zdroje) a sdělení podle čl. 15 až 22 a 34.

Správce musí vždy posoudit důvody, účel a povahu konkrétního zpracování a posoudit, zda a který z právních důvodů lze na dané zpracování použít. Ze shora uvedeného dále vyplývá, že subjekt údajů by měl od správce dostávat relevantní, srozumitelné a přesné informace a správce by ho neměl ohledně zpracování uvést v omyl.

Smlouva je dvoustranné (příp. vícestranné) právní jednání a k jejímu uzavření je třeba, aby s jejím obsahem souhlasily všechny strany smlouvy. Naopak souhlas se zpracováním osobních údajů je projevem vůle pouze dotčeného subjektu údajů a je tedy jednostranným právním jednáním. Proto např. o odvolání souhlasu rozhoduje výlučně subjekt údajů a postoj správce nemá na platnost takového odvolání žádný vliv.

Uvádět souhlas, který je jednostranným právním jednáním ve smlouvě, může být pro subjekt údajů matoucí a může vzbudit dojem, že s odvoláním souhlasu musí souhlasit i druhá strana smlouvy – tedy správce osobních údajů. Nepodmíněnost souhlasu řeší čl. 7 odst. 4.

GDPR s cílem chránit subjekty údajů upravuje uvedenou problematiku v čl. 7 odst. 2 GDPR, který pod sankcí neplatnosti stanoví, že v případě souhlasu vyjádřeného písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný.

Dále čl. 5 odst. 1 písm. c) GDPR stanoví, že shromažďované osobní údaje mají být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Čl. 9 odst. 1 GDPR Zpracování zvláštních kategorií osobních údajů, výslovně zakazuje zpracování konkrétních citlivých údajů (např. náboženské vyznání), pokud není splněn v odst. 2 (Čl. 9) určený účel zpracování.

Se zvláštními kategoriemi osobních údajů je vždy nezbytné pracovat s mimořádnou péčí.

Zjištění a doporučení:

6/1	**Souhlas se zpracováním OÚ – chybná formulace**
Zjištění:	Souhlas se zpracování OÚ má Město sice vytvořený, využívá ho v různém znění na různých formulářích či jiné dokumentaci, ale jeho znění neodpovídá požadavkům GDPR dle čl. 13 a čl. 14 GDPR a čl. 15 až 22 a 34.
Doporučení 1:	Aktualizovat a změnit formulaci souhlasu se zpracováním osobních údajů tak, aby ve všech ohledech reflektovalo novou právní úpravu (vč. odkazu na GDPR místo odkazu na ZOOÚ). Souhlas s odkazem na ZOOÚ lze používat pouze do 24.5.2018, dále již ne. Nový souhlas nechat podepsat všemi subjekty osobních údajů, u kterých je to třeba.
6/2	**Souhlas se zpracováním OÚ pro mzdové a personální účely je součástí osobního dotazníku**
Zjištění:	Auditoři zjistili, že organizace vyžaduje souhlas se zpracováním osobních údajů zaměstnanců v souvislosti s personální a mzdovou agendou, pro pracovněprávní účely a pro plnění dalších úkolů uložených zaměstnavateli právními předpisy, a to v dohodě o provedení práce.
Doporučení 1:	Zpracování a uhrazení mezd a odvodů za zaměstnance je povinností zaměstnavatele plynoucí mu z právních předpisů (zejm. zákoník práce, zákon o organizaci a provádění sociálního zabezpečení atd.). Tento účel však může být naplněn teprve po uzavření pracovněprávního vztahu. Odstranit souhlas se zpracováním osobních údajů pro mzdové a personální účely z žádosti o zaměstnání a nahradit ho informačním memorandem.
Doporučení 2:	Vyžádat si a zdokumentovat souhlas zájemce se zpracováním osobních údajů vedených v evidenci uchazečů za účelem kontaktování (pokud evidence uchazeče nepodléhá zákonné povinnosti), aby bylo možné zjistit, zda jeho zájem trvá i poté, co byl z kapacitních důvodů odmítnut.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	V opačném případě dokumenty skartovat/vymazat z IS.
6/3 	**Absence souhlasu se zpracováním OÚ - evidence odmítnutého žadatele o zaměstnání**
Zjištění:	Auditoři zjistili, že Město zpracovává osobní údaje a životopisy uchazečů o zaměstnání, se kterými nebyla po ukončení výběrového řízení uzavřena pracovní smlouva nebo dohoda o činnostech vykonávaných mimo pracovní poměr. Účelem je zjišťování, zda zájem o zaměstnání i nadále a průběžně trvá. Zájemce je tedy zařazen do pořadníku, avšak bez podepsání souhlasu se zpracováním OÚ k uvedeným účelům. Stejně je postupováno také s nevyžádanými žádostmi o zaměstnání či životopisy.
Doporučení 1:	V případě zájmu uchovávat životopis uchazeče o zaměstnání, se kterým nebyla uzavřena pracovní smlouva nebo dohoda o pracích vykonávaných mimo pracovní poměr, vyžádat si a zdokumentovat souhlas s uchováním životopisu přímo v inzerátu nebo bezprostředně po skočení výběrového řízení, a to za účelem případného dalšího oslovení tohoto uchazeče. Ponechání si informací s osobními údaji bez právního rámce či souhlasu samotného subjektu či poté, kdy účel zpracování již pominul, je v rozporu s GDPR. Toto pravidlo platí jak pro listinnou, tak i elektronickou formu životopisů.
Doporučení 2:	Pokud Město obdrží životopis kandidáta na pracovní pozici bez toho, aniž by bylo zveřejněno výběrové řízení, je nutné v případě zájmu si informace ponechat pro další využití získat Souhlas se zpracováním OU. Ponechání si informací s osobními údaji bez právního rámce či souhlasu samotného subjektu či poté, kdy účel zpracování již pominul, je v rozporu s GDPR. Toto pravidlo platí jak pro listinnou, tak i elektronickou formu životopisů.
6/4 	**Absence souhlasu se zpracováním OÚ - fotografování**
Zjištění:	Město pořizuje (a tuto praxi chce výrazně rozšířit) a dále zpracovává: ▶ Fotografie zaměstnanců se souhlasem (nebo dokonce bez něho), který je obdobně jako souhlas se zpracováním osobním údajů (v obecném vyznění) nedostatečný, protože není přesně specifikován.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 1:	V případě zájmu pořizovat obrazové a případně také zvukové záznamy zaměstnance, je nutné si vyžádat a zdokumentovat za tímto účelem souhlas subjektu údajů jako samostatný dokument. Pokud by správce chtěl pořízené obrazové, případně také zvukové, záznamy zveřejňovat, je třeba získat souhlas i k tomuto účelu zpracování. Dále, pokud subjekt údajů dá souhlas se sběrem audio a obrazových záznamů, pak již není nutné dál tento souhlas uvádět/zveřejňovat.
Doporučení 2:	V případě zájmu zpracovávat otisky prstů, je nutné si vyžádat a zdokumentovat za tímto účelem souhlas subjektů údajů jako samostatný dokument.
Doporučení 3:	Vytvořit Souhlas zaměstnance s poskytnutím zvláštní kategorie údajů jako součást standardního souhlasu zaměstnance. Vzhledem k tomu, že se jedná o zvláštní kategorii údajů (citlivé), nelze v tomto případě uplatnit právní základ zpracování nezbytné pro plnění smlouvy dle čl. 6 odst. 1 písm. b) GDPR.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

6.7 Zpracování OÚ a zvláštní kategorie údajů, které nejsou nezbytně nutné

Legislativní rámec:

Dále čl. 5 odst. 1 písm. c) GDPR stanoví, že shromažďované osobní údaje mají být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

Čl. 9, odst. 1 GDPR Zpracování zvláštních kategorií osobních údajů, výslovně zakazuje zpracování konkrétních citlivých údajů (např. náboženské vyznání), pokud není splněn v odst. 2 (Čl. 9) určený účel zpracování.

Se zvláštními kategoriemi osobních údajů je vždy nezbytné pracovat s mimořádnou péčí.

Zjištění a doporučení:

7.	**Zpracování OÚ a zvláštní kategorie údajů, které nejsou nezbytně nutné - zaměstnanci/uchazeči o zaměstnání**
Zjištění:	Auditoři zjistili, že Město, aniž by to bylo pro stanovené účely nezbytné, zpracovává nadbytečné osobní údaje v rozsahu uvedeném v následujících doporučeních. Uvedená zpracování tak jsou podle názoru auditorů v rozporu s čl. 5 odst. 1 písm. c) GDPR. Auditoři pro úplnost upozorňují, že zpracování osobních údajů a zvláštní kategorie OÚ, které nejsou nezbytně nutné pro stanovený účel zpracování, NELZE právně zhojit ani získáním souhlasu k jejich zpracování. Kromě následujících doporučení na tomto místě uvádí auditoři ještě jedno další, a to doplnit do osobního dotazníku nebo pracovní smlouvy povinnost zaměstnance neprodleně informovat zaměstnavatele o jakýchkoliv změnách, které by mohly mít vliv na pracovněprávní vztah a povinnosti z něho vyplývající.
Doporučení 1:	Nevyžadovat osobní údaje a zvláštní kategorie OÚ, které nejsou nezbytně nutné ve vztahu k účelu, pro který mají být zpracovávány (např. pro účely žádosti o zaměstnání).
Doporučení 2:	Nevyžadovat informace o **zdravotním stavu** uchazeče o zaměstnání/zaměstnance nad rámec vyžadovaný zákonem o

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	pracovnělékařských prohlídkách (pokud se nejedná o dotovanou pozici právě na základě zdravotního znevýhodnění). Pro získávání údajů o zdravotním omezení či čestné prohlášení o zdravotní způsobilosti neexistuje žádný zákonný důvod. Uchazeč o zaměstnání či zaměstnanec sám není kompetentní posuzovat svůj zdravotní stav. Tuto problematiku řeší povinné pracovnělékařské prohlídky, a to vstupní nebo další periodické.
Doporučení 3:	Nevyžadovat **rodné číslo** a rodinný stav v Dohodách o provedení činnosti. Rodné číslo lze zpracovávat výhradně u zaměstnanců, a to pro daňové a mzdové účely. **Rodné číslo** zaměstnance nepoužívat jako identifikátor ve smluvních ujednáních, místo toho používat např. identifikační číslo zaměstnance.
Doporučení 4:	Pro zpracování čísla **občanského průkazu**, eventuálně data jeho platnosti neexistuje žádný zákonný důvod, proto je nutné tyto údaje nepožadovat/nezpracovávat.
Doporučení 5:	Nepožadovat informace o **nedokončeném vzdělání**, toto je však možné nahradit probíhajícím vzděláním, v případě zákonného započtu praxe.
Doporučení 6:	Formulace **„Můžete doložit občanskou a soudní bezúhonnost?“** je nevhodná, protože případ, kdy žadatel odpoví NE, ještě nemusí nutně znamenat, že bezúhonný není. Přípustnou variantou je jednoznačná žádost o dodání výpisu z trestního rejstříku. Pro tyto účely platí presumpce neviny, tzn., že dokud nedojde k pravomocnému rozhodnutí ve smyslu „je vinen“, musí být na takovou osobu nahlíženou jako na nevinnou.
Doporučení 7:	Zpracovávat různé **srážky ze mzdy** (např. výživné, životní pojištění, hypotéky apod.), údaje o oddlužení či náhled do insolvenčního rejstříku je nad rámec povinností zaměstnavatele. Jedná se o dobrovolnou pomoc zaměstnavatele, a proto je nutná aktivní součinnost zaměstnance, který by měl mít na správném zpracování vlastní zájem. Zaměstnanec by měl zaměstnavateli podat písemnou žádost o srážku ze mzdy, ve které uvede potřebné údaje v rozsahu nutném pro zpracování. V takovém případě probíhá zpracování osobních údajů na žádost subjektu údajů a není

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	potřebné získávat její další souhlas se zpracováním, postačí splnění informační povinnosti správcem/zpracovatelem OÚ. Stejné je to v případě **rodinných příslušníků a ostatních vyživovaných osob**, proto doporučujeme údaje o nich z dotazníku odstranit. U dětí je pro mzdové a daňové účely možné zpracovávat pouze datum narození (beze jména). Výjimkou je formulář pro potvrzení o neuplatnění nároku na daňový odpočet za vyživované dítě/děti. K vystavení tohoto potvrzení je zaměstnanec povinen předložit rodný list dítěte, nicméně tato skutečnost nezakládá právní důvod k trvalému zpracování rodného čísla dítěte. V neposlední řadě se jedná o povinnost zaměstnavatele udržovat informace a osobní údaje aktuální. Osobní dotazník zaměstnance se mzdovými a daňovými podklady se stává neaktuálním ve velmi krátké době (např. narození dítěte, ukončení splátek atd.), proto je vhodnější uchovávat tyto údaje, pokud je to nezbytné pro mzdové a daňové účely, odděleně např. ve mzdové složce. Výjimkou jsou pouze údaje o soudně nařízené **exekuci**, které je zaměstnavatel povinen zjišťovat dle občanského soudního řádu č. 99/1963 Sb. § 294.
Doporučení 8:	Nezpracovávat údaje o **národnosti**. Jedná se o zvláštní kategorii údajů, pro kterou není právní základ.
Doporučení 9:	**Státní příslušnost** doporučujeme nezjišťovat **v životopise** uchazeče o zaměstnání. Ačkoliv státní příslušnost uchazeče slouží jako podklad pro další postup při uzavření pracovní smlouvy, doporučujeme tento údaj zjišťovat např. při samotném pohovoru a dále ho systematicky nezpracovávat.
Doporučení 10:	**Číslo bankovního spojení** je možné požadovat pouze v případě, kdy je na tento účet převáděna mzda či jiné platby od zaměstnavatele či jsou na základě dohody/smlouvy z tohoto účtu prováděny srážky, např. stravného apod. Znalost čísla bankovního účtu, na který je převáděna mzda ještě nezakládá povinnost, sdělovat toto třetím osobám, např. exekutorům, protože organizace nemá informaci o skutečném majiteli bankovního účtu, kterému by mohla být, v případě jeho obstavení, způsobena újma.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 11:	**Podrobné informace o dalším pracovním poměru či živnostenském oprávnění** nejsou vyžadovány oprávněně, pokud nejsou kontraindikací k uzavření pracovněprávního vztahu či nezpůsobují střet zájmů vzhledem k povaze vykonávané funkce/pozice. Pro daňové účely lze zjišťovat pouze, zda zaměstnanec má/nemá jiný pracovní poměr či výdělečnou činnost. Další údaje jsou nepřípustné.
Doporučení 12:	**Výši přiznaného důchodu** nelze doložit žádným právním titulem. Lze se dožadovat pouze sdělení ve smyslu zákona č. 582/1991 Sb.: ▶ § 37 písm. g) o starobním důchodu podle § 31 zákona o důchodovém pojištění, kdo jej vyplácí, datum vzniku nároku, popř. číslo rozhodnutí o jeho přiznání, pokud je vyplácen orgány ministerstev obrany, vnitra a spravedlnosti; ▶ § 41 o přiznání předčasného důchodu dle § 31 zákona o důchodovém pojištění; ▶ a dále sdělení o přiznání invalidního důchodu a jeho stupně.
Doporučení 13:	Vyžadování informace o **počtu vychovaných dětí** se řídí § 32 zákona o důchodovém pojištění a je možné pouze u žen s datem narození do roku 1971.
Doporučení 14:	**Oddlužení a náhled do insolvenčního rejstříku** nemá pro paušální vyžadování od všech zaměstnanců oporu v zákonném titulu dle GDPR.
Doporučení 15:	Otázka **„Je proti vám vedeno soudní řízení?“** je nepřijatelná. Pro tyto účely platí presumpce neviny, tzn., že dokud nedojde k pravomocnému rozhodnutí ve smyslu „je vinen“, musí být na takovou osobu nahlíženou jako na nevinnou.
Doporučení 16:	Pro zjišťování rodinného stavu neexistuje právní základ, proto doporučujeme tento údaj o uchazečích o zaměstnání či o zaměstnancích dále nezjišťovat.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

6.8 Pořizování kopií osobních dokladů

Legislativní rámec:

Čl. 5, odst. 1, písm. c) GDPR uvádí, že osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

Na zacházení s osobními doklady se vztahují další zákony v platném znění, např. Zákon o občanských průkazech, Zákon o cestovních dokladech apod.

Zjištění a doporučení:

8/1		**Neoprávněně pořizování fotokopií občanských průkazů**
Zjištění:		Město získávalo od svých zaměstnanců fotokopie občanských průkazů, a tak také přístup k údajům, které není oprávněno získávat a které mohou být zneužity, pokud dojde k selhání jejich fyzické ochrany. Nikdo nemá právo ofotit si jakýkoliv identifikační doklad, přiměřený rozsah osobních údajů lze opsat přímo z tohoto dokladu při uzavírání smlouvy.
Doporučení 1:		Opustit praxi pořizování fotokopií OP zaměstnanců a vkládat je do jejich osobní složky. Potřebné údaje pouze ověřit na základě identifikačního dokladu zaměstnance (nemusí jím být nutně pouze OP).
8/2		**Neoprávněně pořizování fotokopií rodných listů**
Zjištění:		Město získávalo od svých zaměstnanců fotokopie rodných listů dětí zaměstnanců pro daňové účely. Tyto kopie není oprávněno získávat. U dětí je pro mzdové a daňové účely možné zpracovávat pouze datum narození (beze jména). Výjimkou je formulář pro potvrzení o neuplatnění nároku na daňový odpočet za vyživované dítě/děti. Pokud dojde k selhání jejich fyzické ochrany, pak mohou být zneužity. Nikdo nemá právo ofotit si jakýkoliv identifikační doklad, přiměřený rozsah osobních údajů lze opsat přímo z tohoto dokladu.
Doporučení 1:		Opustit praxi pořizování fotokopií rodných listů dětí zaměstnanců a vkládat je do jejich osobní složky. Potřebné údaje pouze ověřit na základě předloženého rodného listu.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

6.9 Aktualizace spisů, stanovení a dodržování skartační lhůty

Legislativní rámec:

Čl. 5, odst. 1, písm. d) GDPR uvádí, že osobní údaje musí být přesné a v případě potřeby aktualizované a musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelu, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.

Ve smyslu zákona č. 499/2004 Sb., o archivnictví a spisové a službě musí být stanovené archivační a skartační lhůty.

Zjištění a doporučení:

9.		**Neprovádění aktualizace spisů a nestanovení/nedodržování skartační lhůty - zaměstnanci/uchazeči o zaměstnání**
Zjištění:		Auditoři zjistili, že Město neprovádí důslednou a pravidelnou aktualizaci spisů/složek v následujícím rozsahu a tím pádem uchovává osobní údaje (dokumenty) poté, co účel zpracování již pominul: ▶ veškerý obsah osobních spisů současných i bývalých zaměstnanců, aniž by byla provedena selekce dokumentů (osobních údajů), které je třeba ihned po skončení pracovněprávního vztahu zlikvidovat, a ▶ životopisy uchazečů, se kterými nebyla uzavřena pracovněprávní smlouva nebo dohoda o práci vykonávané mimo pracovní poměr. Bylo zjištěno, že neprobíhá pravidelná průběžná kontrola nadbytečného či neaktuálního obsahu osobního spisu zaměstnance/uchazeče o zaměstnání.
Doporučení 1:		Prověřit, zda jsou skutečně všechny druhy listin ošetřeny v rámci spisového skartačního řádu na jedné straně. Na druhé straně, zda nejsou dlouhodobě uchovávány dokumenty, u nichž to žádný právní rámec nevyžaduje a neexistuje ani objektivní provozní nutnost k jejich uchovávání (a ani nejsou zmíněny ve skartačním řádu).
Doporučení 2:		Po skončení pracovněprávního vztahu zlikvidovat dokumenty, jejichž další uchování nepožaduje právní předpis (zaměstnavatel musí po stanovenou dobu uchovat stejnopisy evidenčních listů, záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění) nebo jejichž další uchování není v souladu s oprávněnými zájmy správce (např. v případě vysokého rizika soudního sporu s bývalým zaměstnancem).

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 3:	V případě uchazečů o zaměstnání platí ustanovení GDPR o aktuálnosti a aktualizaci ve stejném rozsahu. Proto je nutné zlikvidovat dokumenty, pro jejichž další uchovávání neexistuje právní titul zpracování.
Doporučení 4:	Stanovit skartační lhůty pro uchování jednotlivých dokumentů, které jsou součástí dokumentace o zaměstnanci/uchazeči o zaměstnání.
Doporučení 5:	Platí to i pro spisovou službu a následné dodržování ustanovení Spisového a skartačního řádu.

6.10 Úprava vztahu se zpracovatelem osobních údajů

Legislativní rámec:

Podle čl. 28 odst. 3 GDPR se vzájemný vztah mezi správcem a zpracovatelem osobních údajů řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Smlouva musí dále upravovat např. povinnost postupovat při zpracování podle pokynů správce, povinnost mlčenlivosti osob zpracovávajících osobní údaje pro zpracovatele a povinnost být správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů.

Povinnost uzavřít se zpracovatelem smlouvu vyplývá správci z aktuálně účinného § 6 ZOOÚ. Podle tohoto ustanovení musí správce uzavřít se zpracovatelem smlouvu o zpracování osobních údajů, která bude upravovat v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá. Smlouva musí obsahovat také záruky zpracovatele o technickém a organizačním zabezpečením ochrany osobních údajů.

Zjištění a doporučení:

10/1 	**Nedostatečně upravený vztah se zpracovatelem osobních údajů**
Zjištění:	Bylo zjištěno, že Město má nedostatečné upravené vztahy se zpracovateli osobních údajů, kterými je správcem.
Doporučení:	Doplnit uzavřené smlouvy s externími firmami pomáhající zajistit provoz IT a dalšími zpracovateli osobních údajů. Ve smlouvě se zpracovatelem osobních údajů je nutno zapracovat bezpečnostní požadavky tak, aby vše bylo v souladu s GDPR. Jde zejména o požadavky na dodržení závazku mlčenlivosti všemi pracovníky dodavatele, zachování a dodržování bezpečnostních požadavků zadavatele, závazek přijmutí potřebných zásad pro ochranu osobních údajů, bezpečný způsob práce s paměťovými

	médii včetně jejich bezpečné likvidace apod. a zajištění podpory Správce osobních údajů při plnění legislativních požadavků (například dle GDPR právo subjektu na aktualizaci OU, výmaz, přístup k OU a podobně.). Toto platí pro smluvní ujednání s dodavateli s přístupem k osobním údajům (správa serveru, tak i správy a provozu IT). Znění písemné smlouvy musí vycházet z čl. 28 odst. 3 GDPR a musí obsahovat zejm.: ▶ předmět a dobu trvání zpracování ▶ povahu a účel zpracování ▶ typ osobních údajů a kategorie subjektů údajů ▶ - povinnosti a práva správce a povinnosti a práva zpracovatele, např. povinnost zpracovávat osobní údaje pouze na základě pokynů správce, povinnost zajistit mlčenlivost osob, které se na zpracování podílejí, povinnost zpracovatele přijmout bezpečnostní opatření, povinnost poskytnout součinnost správci při vyřizování požadavků uplatněných subjekty údajů u správce Toto platí pro smluvní ujednání s dodavateli mzdových služeb, tak i správy a provozu IT a dalších. Zároveň je nutné ve smlouvě stanovit také dosažitelnost/dostupnost služeb v případě nedostupnosti klíčových pracovníků dodavatele.

6.11 Fyzická bezpečnost

Legislativní rámec:

Podle čl. 24 odst. 1 GDPR je správce povinen zavést vhodná technická a organizační opatření k zajištění, že zpracování osobních údajů bude v souladu s požadavky GDPR a osobní údaje budou řádně zabezpečeny. Tato opatření je správce povinen zavést zejména s ohledem na rizika pro práva a svobody subjektů údajů.

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku. Podle odst. 2 předmětného ustanovení se při posuzování vhodné úrovně zabezpečení zohlední zejm. rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Podle bodu A.11.1 mezinárodně uznávaného standardu ISO/IEC 27001 vrcholové vedení organizace zavede opatření k zabránění neoprávněného fyzického přístupu, poškození a zasahování do informací, které organizace zpracovává, včetně osobních údajů, a zařízení, kde jsou tyto informace uloženy a zpracovávány. Součástí takových opatření je např. stanovení fyzického ochranného perimetru, kontrola osob při vstupech do vymezeného perimetru (např. kontrola na recepci nebo vrátnici), fyzické zabezpečení místností (např. uzamčení místností, kde jsou umístěny chráněné informace nebo zařízení).

Zjištění a doporučení:

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

11.		Nedostatečná fyzická bezpečnost - listinné a elektronické dokumenty
Zjištění:		Bylo zjištěno, že Město nemá dostatečně zajištěnou fyzickou bezpečnost listinných a elektronických dokumentů obsahujících osobní údaje ve všech jeho budovách a prostorách. Listinné dokumenty jsou uchovávány v neuzamčených či neuzamykatelných policích, skříních či registraturách v kancelářích, do kterých se mohou dostat i návštěvníci Města, některé jsou vyvěšeny na nástěnkách či ponechávány volně ložené na pracovních stolech po delší dobu, než je nezbytně nutné pro jejich zpracování. PC některých uživatelů nejsou při opuštění pracovního místa vždy důsledně zaheslovány, uživatelé se z IS neodhlašují nebo je místnost volně přístupná neoprávněným osobám. PC některých uživatelů jsou při odchodu ze zaměstnání zapnuty, aby bylo možné připojit se vzdáleným přístupem. Do budovy, která má na jedné straně vchod přes čip, je možné vstoupit i z jiného vchodu, kde je sice fyzicky přítomna zaměstnankyně recepce, ale není tím vyloučena možnost náhodného vniknutí do budovy.
Doporučení 1:		Zmapovat a oklasifikovat z hlediska kritičnosti (z pohledu ochrany osobních údajů) jednotlivé budovy/místnosti (perimetry) a uvést bezpečnostní opatření na jejich ochranu. Jde zejména o budovy, kde jsou dlouhodobá uložiště/spisovny.
Doporučení 2:		Stanovit pravidla, popsat způsoby fyzického zabezpečení pro práci s dokumenty, které obsahují osobní údaje (ukládání v uzamykatelných skříních, umístění klíčů, zamykání kanceláří, spořiče obrazovek, odhlašování z PC při opouštění místnosti apod.). Požadavek = jednoznačně uložit do uzamykatelné skříně či registratury. Klíč má být pouze u oprávněné osoby. Při opouštění místnosti/kanceláře, kde je agenda uchovávána platí uzamknout dveře, neponechávat volně na stole či jinde položené složky či jednotlivé dokumenty vyjmuté z registratury či připravené k založení, aby k nim nemohla získat přístup neoprávněná osoba.
Doporučení 3:		Stanovit způsob zajištění přístupu odpovědným osobám.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 4:	Definovat procesy pro vyhodnocování stanovených bezpečnostních opatření.
Doporučení 5:	Doporučujeme, aby pracoviště mělo stanoven řád upravující přístup neautorizovaných osob do objektů. Může jít o úpravu návštěvního řádu tak, aby stanovil povinnost, že návštěvy musí být vždy zaevidované či doprovázeny zaměstnancem Města. Dveře, kterými se přistupuje do prostor organizace zabezpečit koulí z vnější strany tak, aby nikdo nemohl bez klíče či pomoci zaměstnance organizace tam vstoupit.

6.12 Bezpečnost - oblast IT

Legislativní rámec:

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku. Podle odst. 2 daného ustanovení se při posuzování vhodné úrovně zabezpečení zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Podle části 5.2 mezinárodně uznávaného standardu ISO/IEC 27001 vrcholové vedení organizace zavede zdokumentovanou politiku (pravidla) bezpečnosti informací. Součástí těchto pravidel by měly být také pravidla upravující rozsah přístupových oprávnění jednotlivých zaměstnanců k informacím a k zařízením, kde jsou informace, včetně osobních údajů, uloženy a zpracovávány (bod A.9 ISO/IEC 27001). Vrcholové vedení by tak mělo stanovit např. jednotná pravidla pro zajištění kvality hesel a zavést technická opatření vynucující automatizované uplatňování stanovených pravidel (např. příslušná aplikace bude v pravidelných intervalech vyžadovat změnu hesla, nové heslo musí mít definovaný počet a strukturu znaků).

Zjištění a doporučení:

12/1		**Bezpečnost IT - dokumenty s OÚ uložené na lokálním disku PC**
Zjištění:		Mnozí pracovníci si nechávají potřebné či nepotřebné soubory pro další použití na lokálním disku svého PC.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Doporučení 1:	Doporučením je používat centrální úložiště ve formě sdílených složek na serveru. Vyjma zvýšené bezpečnosti to usnadní i proces zálohování.
12/2	**Bezpečnost IT - sdílení hesel do IS/aplikací/PC**
Zjištění:	V Podatelně je využito pouze jedno heslo pro všechny uživatele – skenování dokumentů.
Doporučení 2:	Mezi základní bezpečnostní zásady, odvozeno od rozdělení pravomocí a odpovědností, patří to, že každý je odpovědný za své aktivity a k tomu musí mít k dispozici i odpovídající prostředí. Sem spadá i to, že každý je jediným znalým přístupového hesla ke svému účtu. Proto tato zásada musí být uvedena nejen ve standardech, ale naplňována i v praxi.
12/3	**Bezpečnost IT - nedostatečné zálohování**
Zjištění:	Zálohování osobních počítačů jednotlivých uživatelů není prováděno, ani jinak vynucováno.
Doporučení 3:	K základním požadavkům patří i zajištění dostupnosti služeb. Nastavený systém zálohování tomu neodpovídá. Zálohován by neměl být jen server, ale i všechna zařízení pro chod Města s kritickými aplikacemi, daty. Místo, kam budou zálohy ukládány, musí být bezpečné a musí být pod přímou kontrolou Města či subdodavatelů IT služeb. Tedy by se nemělo jednat o veřejný cloud nebo cloud umístěný v zemi, ve které nelze uplatňovat práva české či EU legislativy.

6.13 Aktuální bezpečnostní hrozby a provádění testů zranitelnosti ICT

Legislativní rámec:

Podle čl. 32 odst. 1 GDPR písm. b) a d) je správce povinen zavést vhodná technická a organizační opatření, aby zajistil, že zpracování osobních údajů bude v souladu s požadavky GDPR.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Zjištění a doporučení:

13/1		**Nesledování aktuálních bezpečnostních hrozeb a neprovádění testů zranitelnosti ICT**
Zjištění:		Bylo zjištěno, že Město neprovádí testy zranitelnosti, které by odhalily silné a slabé stránky ICT infrastruktury, aplikací a dat. Existuje tak riziko, že nebudou odhaleny a odstraněny zranitelnosti, které by mohl potenciální vnitřní nebo vnější útočník využít např. k narušení dat, včetně osobních údajů.
Doporučení:		Sledovat aktuální bezpečnostní situaci, potenciální hrozby a pravidelně provádět testy zranitelnosti.

6.14 Komunikační kanály

Legislativní rámec:

Čl. 32 odst. 1 GDPR stanoví, že správce provede vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku. Podle odst. 2 daného ustanovení se při posuzování vhodné úrovně zabezpečení zohlední zejm. rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Zjištění a doporučení:

14.		**Komunikační kanály – nezabezpečená e-mailová komunikace**
Zjištění:		Auditoři zjistili, že Město nemá dostatečně zpracovanou směrnici upravující používání komunikačních kanálů pro přenos dokumentů obsahujících osobní údaje jak v rámci Města, tak i mimo něho. Město využívá v omezené míře pro předávání dokumentů obsahujících osobní údaje nezašifrovaný e-mail, a to zejména v komunikaci s: ▶ Policií ČR, ▶ Úřadem práce. Osobní údaje jsou posílány přímo v těle zprávy nebo v přiložených souborech, ale bez použití heslování.
Doporučení 1:		Vypracovat komplexní směrnici upravující používání komunikačních kanálů pro přenos dokumentů obsahujících osobní údaje.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	V rámci stanovených procesů a činností určit, jaké komunikační kanály mohou být použité pro předávání osobních údajů jak v rámci organizace, tak i mimo ni. Mezi platné komunikační kanály patří i e-mailová komunikace, ta ale bez dalších technických opatření (šifrování či nastavení ochranou heslem) nesmí být používána pro předávání osobních údajů.

6.15 Analýza rizik pro práva a svobody subjektů údajů

Legislativní rámec:

Podle čl. 24 odst. 1 GDPR je správce povinen zavést vhodná technická a organizační opatření k zajištění, že zpracování osobních údajů bude v souladu s požadavky GDPR a osobní údaje budou řádně zabezpečeny. Tato opatření je správce povinen zavést zejm. s ohledem na rizika pro práva a svobody subjektů údajů.

Povinnost provádět analýzu rizik v souvislosti se zpracováním osobních údajů lze dovodit i z aktuálně účinného § 13 ZOOÚ.

Zjištění a doporučení:

15.		**Neprovádění analýzy rizik pro práva a svobody subjektů údajů a krizového plánu**
Zjištění:		Město neprovádí analýzu rizik pro práva a svobody subjektů údajů a následný krizový/havarijní plán.
Doporučení 1:		Vypracovat analýzu rizik. Může být v jakékoliv formě, formátu. Analýza rizik by měla přinést odpověď na otázku působení jakých hrozeb je společnost vystavena, jak moc jsou její aktiva vůči těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba zneužije určitou zranitelnost a jaký dopad by to na společnost mohlo mít. V analýze rizik se používají následující pojmy: ▶ aktivum (asset) – vše co má pro společnost nějakou hodnotu a mělo by být odpovídajícím způsobem chráněno, ▶ hrozba (threat) – jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	▶ zranitelnost (vulnerability) – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou. ▶ riziko – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti. ▶ opatření (countermeasure) – opatření na úrovni fyzické logické nebo administrativní bezpečnosti, které snižuje zranitelnost a chrání aktivum před danou hrozbou.
Doporučení 2:	Vypracovat havarijní/krizový plán, který by řešil situace vyplývající z analýzy rizik.

6.16 Vnitřní úpravy povinností mlčenlivosti

Legislativní rámec:

Zaměstnanci správce, kteří přicházejí do styku s osobními údaji u správce, jsou povinni zachovávat mlčelivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Tato povinnost by měla trvat i po skončení zaměstnání. Povinnost mlčenlivosti zaměstnanců lze dovodit také z čl. 28 odst. 3 písm. b) ve spojení s čl. 32 odst. 1 GDPR nebo v případě zpracování zvláštní kategorie osobních údajů (citlivých údajů) poskytovatelem sociálních služeb podle čl. 9 odst. 3 GDPR.

S ohledem na zajištění povědomí zaměstnanců o důležitých povinnostech a nedostatečné vymezení povinnosti mlčenlivosti v GDPR by měl správce osobních údajů tuto povinnost zakotvit do pracovněprávních smluv svých zaměstnanců.

Toto se týká všech pracovněprávních vztahů vč. uklízeček, DPP, rámcových smluv, OSVČ apod. a dále všech pověřených zpracovatelů osobních údajů správce vč. dodavatelů IS, kteří provádějí servis a údržbu těchto systémů.

Zjištění a doporučení:

16/1	**Nedostatečná vnitřní úprava povinností mlčenlivosti**
Zjištění:	Město má ošetřenou povinnost mlčenlivosti ve vybraných dokumentech, nicméně lze doporučit úpravu znění povinnosti mlčenlivosti tak, aby obsahovalo tuto povinnost komplexně.
Doporučení:	Do dohod mezi zaměstnavatelem a zaměstnancem doplnit například následující text. Nemusí to být součástí pracovní smlouvy, ale může to být součástí interních směrnic, na které se pracovní smlouva odkazuje. (1) Zaměstnanec se zavazuje zachovávat mlčenlivost o všech skutečnostech, které nejsou veřejně známy a o kterých se dozví v souvislosti s výkonem práce pro zaměstnavatele nebo které mu budou v

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	průběhu výkonu práce zpřístupněny, jakož i o samotné existenci těchto skutečností. Povinnost mlčenlivosti se vztahuje na všechny údaje, včetně osobních, získaných z jakýchkoliv zdrojů, dokumentů a databází zaměstnavatele, klientů a obchodních partnerů zaměstnavatele a jejich klientů, zejména o informacích, poznatcích a skutečnostech, které slouží k dosažení nebo prosazování cílů uvedených subjektů, a to jak v tuzemské, tak i v zahraniční oblasti. (2) Povinnost podle odstavce 1 se vztahuje také na bezpečnostní opatření, jejichž zveřejnění by ohrozilo bezpečnost informací, včetně osobních údajů. (3) Zachovávat mlčenlivost se zaměstnanec zavazuje nejen po dobu trvání pracovněprávního vztahu, ale i po jeho skončení a bere na vědomí, že při porušení povinnosti mlčenlivosti by na něm zaměstnavatel mohl uplatňovat náhradu škody, která by v souvislosti s porušením této povinnosti vznikla.

6.17 Školení - personální bezpečnost a zvyšování bezpečnostního povědomí zaměstnanců

Legislativní rámec:

Podle čl. 24 odst. 1 GDPR je správce povinen zavést vhodná technická a organizační opatření, aby zajistil, že zpracování osobních údajů bude v souladu s požadavky GDPR. Tato povinnost v sobě zahrnuje i prokazatelné proškolování v oblasti bezpečnosti osobních informací. Jedním z předpokladů dosažení souladu s povinnostmi stanovenými GDPR je získání a udržování zdrojů nutných pro řádné fungování systému bezpečnosti informací (bod 7.1 ISO/IEC 27001). Mezi uvedené zdroje patří také dostatečné kvalifikovaný personál vykonávající činnosti, které ovlivňují úroveň bezpečnosti informací.

Zjištění a doporučení:

17/1		**Školení - Neprovádění systematického zvyšování povědomí o ochraně osobních údajů a o jejich zabezpečení**
Zjištění:		Bylo zjištěno, že Město nevyvíjí systematické aktivity podporující zvyšování povědomí zaměstnanců o ochraně osobních údajů. Absence cílených aktivit zvyšování povědomí o ochraně osobních údajů a jejich zabezpečení představuje riziko pro zvládnutí povinností plynoucích z GDPR a s tím související reputační riziko.
Doporučení 1:		Naplánovat a realizovat, např. také v pracovním řádu či jinde, aktivity směřující k zvyšování povědomí zaměstnanců o ochraně osobních údajů

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	a jejich zabezpečení, např. vstupní školení a pravidelně opakující se přednášky a semináře, tyto aktivity dokumentovat.
Doporučení 2:	V samotném školení pak zmínit zásady bezpečného chování uživatelů z níže uvedených oblastí bezpečnostního desatera. ▶ Každý pracovník nese odpovědnost za ochranu zařízení jak na svém pracovišti, tak i mimo něj. ▶ Musí být přijata adekvátní opatření pro ochranu osobních údajů v rámci fyzické ochrany. ▶ Každý pracovník musí chránit své bezpečnostní a osobní údaje (hesla, kódy PIN, přístupové kódy, apod.), nikomu je nesdělovat, hesla pravidelně měnit. ▶ Na zařízení smí být používán pouze podporovaný SW včetně operačního systému a internetového prohlížeče), musí být vždy bezprostředně aplikovány bezpečnostní update/patche a používat aktuální antivirové a anti-spyware programy s nastavenou on-line ochranou. ▶ Připojení přes Internet prostřednictvím firewallu a pouze přes prověřená datová spojení včetně WI-FI sítí. ▶ Nestahovat z internetu a ani z jiných zdrojů neznámé soubory, příp. programy. ▶ Pozor na nedůvěryhodné e-maily (zprávy od neznámých odesílatelů, případně zprávy s podezřelým názvem či obsahem), neotvírat a bez otevření mazat. ▶ Ověřit platnost certifikátu stránky. ▶ Při jakémkoliv podezření na možnost zneužití svých přístupových údajů do služeb a na stránky, které uživatel používá, ihned službu buď zablokovat či změnit přístupové údaje. ▶ Citlivá data včetně osobních údajů mohou být jen na schválených úložištích a zařízeních.

6.18 Povinnost jmenovat pověřence pro ochranu osobních údajů

Legislativní rámec

Podle čl. 37 odst. 1 písm. a) je správce a zpracovatel povinen jmenovat pověřence pro ochranu osobních údajů, pokud je tento správce a zpracovatel veřejným subjektem.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Město bude s nabytím účinnosti GDPR povinna pověřence pro ochranu osobních údajů zajistit.

Zjištění a doporučení:

18.		**Povinnost jmenovat pověřence pro ochranu osobních údajů**
Zjištění 1:		Město jmenovalo pověřence pro ochranu osobních údajů v dostatečném předstihu před nabytím účinnosti GDPR. Město vhodně zvolilo využití odboru Interní audit pro tuto povinnost, kdy předešlo možnému střetu zájmu tím, že DPO byla jmenována vedoucí tohoto odboru a zároveň si zajistilo (nejen zástupnost) dostatečné profesionální zabezpečení jmenováním právníka do této pozice.
Doporučení 1:		Bez doporučení

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

7. ZJIŠTĚNÍ PRO JEDNOTLIVÉ ODBORY MĚSTA

7.1 Odbor dopravních a správních činností

1. Při projednávání přestupků může dojít k situaci, kdy celý rozhovor, včetně osobních údajů může vyslechnout jiný úředník.

2. Vydané rozhodnutí je postoupeno na odbor ekonomiky k dalšímu řízení. Toto rozhodnutí jde kompletní včetně popisu přestupku (může obsahovat osobní údaje přestupce i jiných lidí).

3. Při běžné činnosti zůstávají spisy jednotlivých případů otevřené na pracovních stolech, včetně osobních údajů. K těmto spisům může mít přístup neočekávaná návštěva, ať to je jiný úředník města, případně kdokoliv jiný.

4. Při projednávání téměř všech agend Odboru jsou získávány kontaktní údaje na účastníky řízení, žadatele apod. Někdy se získávají i osobní údaje jiných osob, např. zplnomocněných zástupců, příbuzných apod., které jsou nad rámec zákonem vyžadovaných údajů a oprávněnost jejich získávání musí být doložena.

5. Odbor zajišťuje i sběr údajů, včetně osobních pro výkon státní správy. Při tomto respektuje požadavky jednotlivých aplikací či databází. Toto je prováděno v dobré víře, že všechny požadavky státní správy jsou v souladu se zákonem včetně GDPR.

6. Některé požadavky státních institucí obsahující osobní údaje jsou na Odbor zasílány nezabezpečeným mailem (např. Policie ČR, soudy apod.).

7.2 Odbor ekonomiky

1. Při zveřejňování tzv. transparentních účtů jsou viditelné osobní údaje jak majitele (zřizovatele) účtu, tak i jednotlivých vkladatelů. Toto je dané současným stavem a systémem správy účtů a v případě zjištění ÚOOÚ ho musí řešit jednotlivé bankovní instituce a nikoliv Odbor. Není ani nutné „začerňování“ osobních údajů při dalším využití údajů a výpisů z těchto transparentních účtů.
2. Úředníci Odboru mohou při zpracování svých agend vidět osobní data zpracovaná v jednotlivých dokumentech, která nejsou potřebná pro jejich práci (např. jednotlivé předpisy plateb).

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

7.3 Odbor rozvoje a investic

1. Při návštěvách Odboru se případný návštěvník nahlásí na recepci a ta pouze ověřuje, zda je na Odboru někdo přítomen. Není vyžadováno vyzvednutí návštěvníka a tím i zajištění kontroly nad pohybem této osoby v budově Města.

2. Při zajišťování vyjádření účastníků řízení např. ke stavbě z hlediska územního plánu, je nejčastěji využito pouze jméno a příjmení pro zajištění totožnosti dotčené osoby. V některých případech jsou však na Odbor předávány i jiné osobní údaje (např. kontaktní), které pak následně musí Odbor zpracovávat v souladu se zákonem.

3. Odbor velmi často zpracovává osobní údaje fyzických osob – podnikatelů. V tomto případě je potřebné rozlišit agendu, ke které se tyto údaje vztahují a podle toho rozhodnout o způsobu jejich zpracování.

7.4 Odbor stavební úřad

1. Při přijímání všech typů žádostí zpracovává Odbor osobní údaje žadatele, včetně kontaktních a to na něho samotného nebo na jiné pověřené či zplnomocněné osoby. V těchto případech je nutné zvážit rozsah kontaktních údajů tak i rozsah osob, jejichž údaje jsou získávány.

2. Odbor zveřejňuje na úřední desce informace o průběhu jednotlivých řízení. V těchto případech používá u žadatele osobní údaj „rok narození“ jako identifikátor zabraňující možným problémům osob se stejným jménem. U sousedů, účastníků řízení tento údaj využíván není, což naopak problém identifikace způsobit může.

7.5 Odbor životního prostředí

Nebyly zjištěny žádné potenciální problémy či rizika v dokumentech nebo činnostech Odborem.

7.6 Odbor vnějších vztahů

1. Při zajištění akce „Rodinné zápolení“ dochází ke zpracování osobních údajů získaných:
   a. Na webové stránce www.rodinnezapoleni.cz
   b. Osobně při registraci na akci samotné

2. Je umožněna účast v závodech i těm, kteří neprojdou registrací.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

3. Není získáván souhlas s pořizováním fotografií či videí účastníků akcí.

3. Při akci „Chomutovský půlmaraton“ (1.9.2018) vystupuje Město jako hlavní pořadatel, závod samotný však zajišťuje externí firma. Je nutné prověřit průběh a ochranu osobních údajů účastníků závodu mezi oběma subjekty. Správcem osobních údajů je v tomto případě nepochybně Město.

7.7 Odbor majetku města

1. Při prodeji majetku Města jsou využity formuláře na webových stránkách Města. Je tam použito i rodné číslo žadatele, které je využito až následně při úspěšném prodeji pro registraci návrhu na vklad do Katastru nemovitostí.

2. Komunikace s žadatelem probíhá nezabezpečeným emailem (včetně návrhu smluv, kde jsou osobní údaje).

3. Pro zpracování agendy nájemních smluv je využíváno nadbytečně rodné číslo.

4. Žadatelé jsou prověřování v rámci Města např. pro bezdlužnost. Je potřebné najít buď právní titul, oprávněný zájem Města nebo zajistit souhlas žadatele s využitím jeho osobních údajů pro tuto proceduru.

7.8 Úsek kancelář tajemníka

1. Při zveřejňování výběrových řízení je součástí formuláře i souhlas s použitím a zpracováním osobních údajů. Tento však není nutný, pokud jsou uvedené osobní údaje využity pouze pro potřeby tohoto výběrového řízení.

2. Osobní dotazník zaměstnance je vyplňován před podepsáním pracovní smlouvy. Obsahuje nadbytečné údaje pro uzavření pracovní smlouvy a dále údaje, které jsou potřebné pro zpracování jiných agend (např. mzdová, daňová apod.).

3. Nejsou prováděny pravidelné kontroly a aktualizace osobních spisů zaměstnanců. Zůstávají tam pak dokumenty obsahující osobní údaje pro Město nepotřebné a nadbytečné.

4. Při zpracovávání agendy pro Radu a Zastupitelstvo Města jsou v přípravných dokumentech a následně i v rozhodnutích a usneseních uváděny osobní údaje (např. při prodejích, pronájmech apod.). Není využita žádná možnost anonymizace těchto údajů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

5. Při zpracování exekuční agendy zaměstnanců se tisknou jednotlivé dokumenty a předávají na mzdovou účtárnu. Údaje o exekuci jsou svou povahou „zvláštní kategorií“ údajů a měla by jim být věnována patřičná péče.

6. Jednotliví zastupitelé dostávají hesla do potřebných aplikací a databází Města. Ani tato hesla nejsou měněna a naopak jsou v některých případech uchovávána u jiných zaměstnanců.

7. Osobní údaje zastupitelů se zadávají do ministerského portálů. Jde o zákonné zpracování osobních údajů.

7.9 Odbor informačních technologií

1. Administrátorská práva jsou v rukou zaměstnanců Odboru. V současnosti však stále zůstávají některá administrátorská oprávnění na zaměstnancích jiných odborů. Tato práva jsou jim postupně a kontrolovaně odebírána.
2. Ochrana osobních údajů není formálně nijak stanovena.
3. Odbor nemá žádné pravomoci a odpovědnosti za zajišťování ochrany osobních údajů u organizací zřizovaných Městem.
4. Není prováděno, vyžadováno a ani kontrolováno zálohování lokálních PC.
5. Emailová pošta zaměstnanců úřadu se maže bez pořízení zálohy.
6. Není žádná procedura vynucující změnu hesla pro jednotlivé zaměstnance Města.

7.10 Odbor interní audit

1. Právní úsek
   i. Některé dokumenty jsou v neuzamčených skříních, případně jsou pouze položeny na pracovních stolech.
   ii. Některé agendy útvaru (např. podání žalob, stížnosti apod.) jsou na sdíleném disku Odboru.
   iii. Útvar má k dispozici i spisy k dlouhodobě běžícím řízením (např. exekuce), jejich archivace je tedy obtížná.
   iv. Evidence stížností je vedena pouze na osobním PC v excelu. Je potřebné dbát na zálohování a omezení přístupu osob bez pověření k vyřizování stížností či její kontrole.
   v. Útvar si ukládá na PC interní konzultace jednotlivých případů. Většinově neobsahují osobní údaje. Pro případ, kdyby tomu tak nebylo je nutné i tuto konzultaci poznamenat do záznamu o zpracování osobních údajů.
   vi. Zbytečné osobní údaje (byť poskytnuté v dobré víře) jsou na webu začerňovány a nejsou využity při zpracování odpovědí žadatelům či stěžovatelům.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

2. Interní audit

Nebyly zjištěny žádné potenciální problémy či rizika v dokumentech nebo činnostech Odborem.

7.11 Podatelna

1. Jednotlivé odbory a vedení Města specifikovalo své požadavky na skenování jim příslušných dokumentů – např. sken jen první strany dokumentu, neotvírání obálek, nepořizování skenu osobních dokladů apod. Tato pravidla však nejsou nijak popsána, jsou pouze ústní a zvyklostní.

2. Systém e-spis je využíván od roku 2009, do té doby existuje pouze listinná podoba dokumentů – např. podací deníky, které jsou archivovány.

3. Na pořizování skenů je používáno jedno společné heslo, teprve dle zápisu ze systému e-spis je možné určit, kdo sken dokumentu pořídil a kam ho zařadil.

4. Úklid podatelny je zajištěn bez přítomnosti zaměstnankyň podatelny, klíče od ní má i jedna další zaměstnankyně Města.

5. Do podatelny je pouze jeden fyzický vstup, dveře však nejsou úplně zavřeny, aby si např. zaměstnanci jednotlivých Odborů mohli přijít pro dokumentaci a údržbáři pro svou poštu

6. Přes podatelnu se pohybují i zaměstnanci ochranky.

7. Přejímání a posílání soukromé pošty zaměstnanců se provádí, omezeně, ale není to žádným předpisem zakázáno.

7.12 Pracovní skupina (organizační složka města, právní subjektivita):

1. Pro svou činnost využívá i dotazník pro uchazeče o zaměstnání dle jednotlivých projektů (např. Projekt Prostupné zaměstnávání lidí od 50 do 64 let (garant je MPSV – účastníky zajišťuje i Úřad práce). Dotazník obsahuje jak osobní údaje, tak i údaje zvláštní kategorie např. hobby.
2. Po uzavření smlouvy je prováděna tzv. „bilanční pracovní diagnostika“, která rovněž obsahuje osobní údaje i údaje zvláštní kategorie.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

3. Pro zajištění veřejné prospěšné práce pod Úřadem práce disponuje Město seznamem se jmény a daty narození, píše pracovníkům docházku a osobně ji pak donese na Úřad práce (kontrolu identity provádí správce lokality).
4. Pro obecně prospěšné práce (alternativní tresty), které mohou vykonávat odsouzení a propuštění (pod Mediační a probační službou) je shodný postup jen zajišťovaný jinou agenturou.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

8. PŘÍLOHY

Příloha č. 1: Metodika auditu

Příloha č. 2: Kontextové informace k ochraně osobních údajů

Příloha č. 3: Organizace města

Příloha č. 4: Vzor interní analýzy provedené odbory Města v roce 2017

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Příloha č. 1: Metodika auditu

Metodika BDO pro ověření shody s požadavky GDPR

BDO ve spolupráci s dalšími evropskými pobočkami BDO vyvinulo vlastní metodiku a nástroje, které minimalizují náklady a rizika spojená s problematikou a požadavky GDPR. Compliance audit (ověření shody) je rozdílová analýza, která identifikuje oblasti, které jsou v rozporu s GDPR a související rizika. Společně s identifikací rizik a jejich závažnosti je součástí compliance auditu také návrh optimalizačních opatření.

Audit vychází při compliance auditu z ustanovení GDPR, zákona o ochraně osobních údajů, judikatury a stanovisek orgánů dozoru a standardů řady ISO/IEC řady 27000 upravujících řízení bezpečnosti informací.

Audit zahrnuje:

- prověření vnitřní řídící dokumentace související s ochranou osobních údajů (politiky, směrnice, řády, záznamy, soubory),
- prověření procesů a organizačních a technických opatření souvisejících s ochranou osobních údajů,
- analýzu dat a klasifikaci osobních údajů,
- analýzu zabezpečení dat a přístupových oprávnění,
- prověření dodržování povinností týkajících se ochrany osobních údajů (povinnosti dle GDPR, zákona o ochraně osobních údajů a prováděcích předpisů, kodexů chování a standardů),
- analýzu účelů zpracování osobních údajů a posouzení jeho legitimity ve vazbě na GDPR a
- identifikaci rizik souvisejících s ochranou osobních údajů, včetně klasifikace jejich závažnosti.

Kritéria auditu

Jde o nezávislé ověření shody současného nastavení a fungování procesů a bezpečnostních opatření organizace s požadavky stanovenými GDPR.

Bylo prověřeno plnění následujících požadavků požadovaných při zpracování osobních údajů:

- dodržování zásad zpracování osobních údajů,
- vedení dokumentace systému řízení osobních údajů,

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

- nastavení a fungování organizačních opatření,
- řízení lidských zdrojů z pohledu bezpečnosti osobních údajů,
- nastavení a fungování technických opatření.

Zásady zpracování osobních údajů

GDPR stanoví základní zásady (základní povinnosti), které musí být dodržovány v průběhu zpracování osobních údajů.

Definice osobních údajů

Osobní údaje jsou ve stávající směrnici z roku 1995 i v GDPR definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.

Mezi obecné osobní údaje patří jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresa a fotografický záznam. Mezi osobní údaje patří i tzv. organizační údaje (například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem).

GDPR definuje také zpracování zvláštních kategorií osobních údajů, citlivých osobních údajů. Těmito údaji jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí. Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby nebo z analýzy jiného prvku, která umožňuje získat rovnocenné informace. Mezi osobní údaje o zdravotním stavu musí být zahrnuty veškeré údaje související se zdravotním /duševním stavem.

Biometrickým údajem jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují jedinečnou identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, ale podle poslední judikatury i podpis.

Naopak z působnosti GDPR jsou vyloučeny anonymizované údaje, údaje zemřelých osob a údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter.

Transparentnost zpracování osobních údajů

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Všechny informace a všechna sdělení týkající se zpracování osobních údajů musí být snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků.

Povinnost zpracovávat osobní údaje pouze pro konkrétní a legitimní účely

Osobní údaje mohou být shromažďovány výhradně pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

Minimalizace osobních údajů

Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

Omezení uložení osobních údajů

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.

Zákonnost zpracování osobních údajů

Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným způsobem. Zpracovávat osobní údaje je možné pouze tehdy, pokud existuje alespoň jeden z dále uvedených právních titulů (důvodů) pro zpracování osobních údajů:

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Dokumentace systému řízení osobních údajů

V rámci ověření dokumentace systému řízení osobních údajů se audit zabýval, zda jsou procesy zpracování osobních údajů a související procesy řádně dokumentovány. V této souvislosti byla prověřena existenci bezpečnostní politiky nebo jiných pravidel upravujících zásady ochrany osobních údajů. Bylo též prověřeno, zda je zdokumentováno rozdělení pravomocí a odpovědností za řízení a ochranu osobních údajů. Součástí ověření byla také metodika pro identifikaci a hodnocení aktiv a rizik. Ověřena byla také existence plánů zvládání rizik a plánů pro řízení kontinuity. Předmětem auditu byly i smlouvy se zpracovateli osobních údajů a s třetími stranami.

Organizační opatření

Audit se zabýval nastavením organizačních opatření a ověřil, zda jsou zavedena následující organizační opatření:

- nastavení pravomocí a odpovědností,
- identifikace a evidence aktiv,
- řízení rizik,
- zohledňování vlivu změn v rámci a vně organizace na systém řízení osobních údajů,
- řízení dokumentace,
- Identity Management – řízení životního cyklu uživatelů a úrovně jejich přístupu k osobním údajům,
- procesy pro řízení vztahů se zpracovateli a dalšími dodavateli,
- řízení a zvládání bezpečnostních incidentů,
- plány kontinuity,
- procesy pro komunikaci s Úřadem pro ochranu osobních údajů.

Předmětem auditu bylo také ověření monitoringu a hodnocení účinnosti zavedených organizačních opatření.

Řízení lidských zdrojů z pohledu bezpečnosti osobních údajů

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Tématem auditu bylo i řízení lidských zdrojů z pohledu bezpečnosti osobních údajů. V této souvislosti bylo ověřeno nastavení a fungování procesů pro řízení lidských zdrojů, včetně získávání a výběru zaměstnanců, uzavírání pracovněprávních smluv, motivace a rozvoje lidských zdrojů a také ukončování pracovněprávních vztahů. Audit se také zabýval zajištěním povinnosti mlčenlivosti ve vztahu k osobním údajům.

Technická opatření

Audit se zabýval fungováním technických opatření a ověřil, zda jsou zavedena následující technická opatření:

- nástroje pro řízení přístupových oprávnění,
- nástroje pro ověřování identity uživatelů,
- klíčové hospodářství,
- prostředky pro zamezení neoprávněného přístupu do prostor či k osobním údajům,
- integrita komunikačních cest (např. ochranou a segmentací sítě, jejího oddělení od vnější sítě a řízením přístupů k síti, bezpečné předávání papírové dokumentace),
- používání nástroje pro ochranu před škodlivým kódem,
- nástroje pro zaznamenávání vykonávaných činností a osobními údaji v informačních systémech,
- nástroje pro sledování a vyhodnocování hrozeb v souvislosti s osobními údaji,
- používání kryptografických prostředků.

Postup auditu

Analýza interní dokumentace

V rámci této fáze byly posouzeny vnitřní předpisy, politiky, směrnice, metodiky a další podklady týkající se předmětu auditu. Audit identifikoval procesy zpracování osobních údajů. V rámci posouzení uvedených podkladů byly zhodnoceny nastavení bezpečnostních opatření a rizika pro organizaci i pro subjekty osobních údajů, jak to vyžaduje GDPR.

Ověření procesů a opatření

Audit shromáždil potřebné informace a dokumenty.

Závěr analýzy

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Na základě zhodnocených důkazů a informací byla zpracována zpráva, v které byly shrnuty závěry z auditu včetně navržených opatření.

Zdroje informací

Hlavním zdrojem informací byly obdržené písemné podklady a výstupy z rozhovoru s vybranými pracovníky organizace.

V průběhu auditu byly poskytnuty zejména tyto dokumenty vztahující se ke zpracování osobních údajů:

- Prohlášení o mlčenlivosti;
- Smlouva o poskytnutí sociálních služeb v DS;
- Smlouva o poskytnutí odlehčovacích služeb – pobytová forma;
- Smlouva o poskytnutí sociálně aktivizačních služeb;
- Smlouva o poskytnutí pečovatelské služby.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Příloha č. 2: Kontextové informace k ochraně osobních údajů

Ochrana osobních údajů je zakotvena v ústavě České Republiky.

Usnesení č. 2/1993 Sb. předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku ČR ustanovuje

- právo na nedotknutelnost osoby a jejího soukromí (čl. 7 odst. 1)
- právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života (čl. 10 odst. 2)
- právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě (čl. 10 odst. 3)

Právo ochrany osobních údajů je regulováno i nad zákonnými právními instrumenty. Základním je úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat, vyhlášená pod č. 115/2001 Sb., která pro Českou republiku nabyla účinnosti dne 1. listopadu 2001. Tuto úmluvu doplňuje dodatkový protokol Rady Evropy z 8. listopadu 2001 č. 181 k úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice, vyhlášený pod č. 29/2005 Sb., který pro Českou republiku nabyl účinnosti dne 1. července 2004. V českém ústavním právu je jím výše zmíněný článek 7 odst. 1 a článek 10 odst. 2 a 3 Listiny základních práv a svobod.

Z hlediska Evropské unie je základem článek 16 smlouvy o fungování Evropské unie (TFEU) ve znění Lisabonské smlouvy a článek 8 Charty základních práv Evropské unie. Základem zákonné regulace je směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obsah a účinné znění), která bude od 25. května 2018 nahrazena obecným nařízením o ochraně osobních údajů (GDPR).

Obecným právním předpisem ochrany osobních údajů v ČR je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (účinné znění, obsah), který od 25. května 2018 bude nahrazen GDPR a českým adaptačním zákonem.

Evropský parlament schválil 27. dubna 2016 Obecné nařízení o ochraně osobních údajů („GDPR“). Účinnost tohoto nařízení nastává 25. května 2018. Pro všechny subjekty, které zpracovávají osobní údaje občanů Evropské unie („EU“), znamená toto opatření upřesnění či vznik nových povinností v souvislosti se zvýšením ochrany a práv občanů Evropské unie.

GDPR je vydáno formou přímo účinného nařízení, které není nutno transponovat do právních řádů členských států. V České republice toto nařízení nahradí současnou právní úpravu ochrany osobních údajů. Níže jsou uvedeny změny a jejich dopady, které GDPR vyvolává:

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

- zpřísnění podmínek pro evidenci a zpracování osobních údajů, a to jak ve zcela nebo částečně automatizovaném, tak i v neautomatizovaném zpracování,
- přísnější požadavky na podobu souhlasu se zpracováním osobních údajů od subjektu údajů a výslovně zakotvené právo souhlas odvolat,
- nová práva subjektů údajů jako např. právo na přenositelnost údajů, nebo významné posílení stávajících práv jako např. práva být zapomenut,
- širší informační povinnost – správce je povinen subjekty údajů dostatečně a srozumitelně informovat, např. o účelu a právním základu zpracování osobních údajů, o jejich právech atd.,
- nové požadavky na obsah smlouvy uzavřené mezi správcem a zpracovatelem,
- přísnější požadavky na zabezpečení osobních údajů – i když je nařízení založeno na principu technologické neutrality, zmiňuje možná technická opatření sloužící k ochraně integrity, důvěrnosti a dostupnosti dat,
- povinnost zohledňovat požadavky GDPR již při zavádění nebo úpravě stávajících procesů GDPR (zásada Privacy by design) a aplikace nejpřísnějšího režimu ochrany osobních dat (zásada Privacy by default),
- přísnější nároky na dokumentaci zpracování osobních údajů,
- v případě vysokého rizika pro práva a svobody subjektů údajů musí být zpracováno posouzení vlivu na ochranu osobních údajů („DPIA“),
- požadavek na reportování porušení zásad ochrany dat jak příslušnému orgánu, tak i subjektu údajů,
- ve vybraných případech povinnost jmenovat Pověřence pro ochranu osobních údajů (DPO),
- nařízení upravuje výši sankcí pro organizace při nedodržení podmínek GDPR.

Porušení výše uvedených povinností může vyústit v pokutu ve výši až 20 mil. EUR. Popsané změny musí správci a zpracovatelé osobních údajů zahrnout do svých systémů řízení, firemních (organizačních) procesů včetně úpravy příslušných dokumentací, či provedení úprav dodávaných produktů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Příloha č. 3 - Organizace Města

Organizační složky statutárního města Chomutova:

Městská policie Chomutov

Jednotka sboru dobrovolných hasičů

Centrum komunitního plánování

Podpora handicapovaným

Pracovní skupina

Příspěvkové organizace statutárního města Chomutova:

Městské lesy Chomutov

Podkrušnohorský zoopark Chomutov

Sociální služby Chomutov

Středisko knihovnických a kulturních služeb Chomutov

Technické služby města Chomutova,

Školy a školská zařízení :

Základní škola Chomutov, Zahradní 5265

Základní škola Chomutov, Na Příkopech 895

Základní škola Chomutov, Kadaňská 2334

Základní škola Chomutov, Písečná 5144

Základní škola Chomutov, Hornická 4387

Základní škola Chomutov, Akademika Heyrovského 4539

Základní škola Chomutov, Březenecká 4679

Základní škola a Mateřská škola, Chomutov, 17. listopadu 4728,

Základní umělecká škola T.G.Masaryka, Chomutov

Základní škola speciální a Mateřská škola, Chomutov, Palachova 4881, příspěvková organizace

Mateřská škola Chomutov, příspěvková organizace

Středisko volného času Domeček Chomutov, příspěvková organizace

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Příloha č. 4 - Vzor interní analýzy provedené odbory Města v roce 2017

GDPR – odbor xxxxxxxx – vstupní analýza, kde se setkáváme s osobními nebo citlivými údaji

Verze 1 ze dne 25. 8. 2017

	tvorba a kontrola smluv	žaloby a vymáhání	konzultace	žádosti o výjimku z OZV	evidence pohledávek	evidence smluv
Proč?	zákon, vnitřní směrnice	zákon – určitelnost žalovaného	různé, nelze specifikovat	žádost o výjimku	zákony o účetnictví apod.	vnitřní směrnice, přehled o smluvních vztazích
O kom?	smluvní strana a její zaměstnanci, zaměstnanci města	žalovaný/povinný	různé, nelze specifikovat	žadatel a osoby podílející se na organizování akce	dlužník	smluvní strana a její zaměstnanci, zaměstnanci města
Co?	smlouvy a podklady k nim, komunikace s druhou stranou, usnesení, průvodní list ke smlouvě	předžalobní výzvy, žaloby a podklady k nim, návrhy na exekuci, insolvenční řízení, komunikace s protistranou, dokumenty od soudu, od exekutora, zprávy do RM/ZM	dotazy, podklady, odpovědi	žádost a podklady, usnesení a vyrozumění o výsledku	evidence údajů	evidence údajů + smlouva s průvodním listem
Kdy?	předběžně před uzavřením smlouvy + elektronické podklady uloženy pro další použití v PC, fyzická smlouva vrácena zpracovateli	od předání pohledávky k vymáhání do doby úplného vymožení či odepsání pro nevymahatelnost + archivace	různé, nelze specifikovat, po vyřešení uchováváno v PC pro další využití	od podání žádosti do vyrozumění o výsledku + archivace	od předání pohledávky k vymáhání do doby úplného vymožení či odepsání pro nevymahatelnost	od předání smlouvy do registru smluv + archivace (uchováváme nad rámec zákonné archivační a skartační doby)
Jak?	v e-mailu, uložené v PC, fyzicky s průvodním listem, schvalování přes materiály do RM/ZM (formserver)	v písemné (spis) i elektronické podobě (PC, e-mail, e-spis), v případě prominutí dluhu též zpráva do RM/ZM ve formserveru	e-mail, písemné podklady, ústní informace, uložené v PC, formserver	v písemné nebo i elektronické podobě (e-mail, e-spis, uložené v PC, formserver), zprávy do RM	VITA, GINIS, IR MONITOR	GINIS, fyzický registr smluv
Kdo	zpracovatel, vedoucí odboru, právník, administrativní pracovník, příkazce operace,	předávající odbor, právník, administrativní pracovník, vedoucí odboru, primátor, případně RM a ZM	právník, vedoucí odboru	právník, administrativní pracovník, vedoucí odboru, RM	administrativní pracovník vedoucí odboru právník	administrativní pracovník vedoucí odboru

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	správce rozpočtu, člen vedení města, hlavní účetní, primátor					
Obecné osobní údaje						
Jméno	ANO	ANO	nepravidelně	ANO	ANO	ANO
Pohlaví	nepřímo lze zjistit, účelově nesledujeme					
Věk	nepřímo lze zjistit, účelově nesledujeme					
Datum narození	ANO	ANO	nepravidelně	ANO	ANO	ANO
Rodné číslo	nepravidelně	nepravidelně		NE (výjimečně ano)	ANO	
IP adresa	NE	NE	NE	NE	NE	NE
Fotografický záznam	NE	NE	NE	NE	NE	NE
Organizační údaje						
e-mailová adresa	nepravidelně	nepravidelně	nepravidelně	ANO	NE	nepravidelně
Telefonní číslo	nepravidelně	nepravidelně	nepravidelně	ANO	NE	nepravidelně
Identifikační údaje vydané státem	ANO (IČ)	ANO (IČ)	nepravidelně	ANO (IČ)	ANO (IČ)	ANO (IČ)
Citlivé údaje						
Rasový, etnický původ	NE	NE	NE	NE	NE	NE
politické názory	NE	NE	NE	NE	NE	NE
náboženství	NE	NE	NE	NE	NE	NE
filozofické vyznání	NE	NE	NE	NE	NE	NE
členství v odborech	NE	NE	NE	NE	NE	NE
zdravotní stav	NE	NE (výjimečně ano – žádosti o prominutí dluhu)	NE	NE	NE	NE
sexuální orientace	NE	NE	NE	NE	NE	NE

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

trestní delikty	NE	nepravidelně	nepravidelně	NE	NE	NE
pravomocná odsouzení	NE	nepravidelně	nepravidelně	NE	NE	NE
genetické, biometrické údaje a osobní údaje dětí	NE	NE	NE	NE	NE	NE

Kde vedeme:

1) viz JAK

Mohou nastat i další případy, např.

- výjimka může nastat vždy a osobní či citlivý údaj se objeví i v agendě, kde se obvykle nevyskytuje

dne **vypracoval**

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost