Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Zpráva nezávislého auditora

o ověření shody s požadavky GDPR

město Uherský Brod

Koncepce města – pasporty – strategie – KOMPAS pro Uherský Brod
Strategie ochrany osobních údajů ve veřejné správě
reg. č. CZ.03.4.74/0.0/0.0/16_058/0007427

Datum vyhotovení: srpen 2019

OBSAH

1. SEZNAM ZKRATEK

Zkratka	Vysvětlení zkratky
DPIA	Data Protection Impact Assessment (posouzení vlivu na ochranu osobních údajů)
Město	Uherský Brod
MÚUB/ MěÚ	Městský úřad Uherský Brod
KOMPAS	Projekt „Koncepce města – pasporty – strategie – KOMPAS pro Uherský Brod“ Registrační číslo CZ.03.4.74/0.0/0.0/16_058/0007427“
MP	Městská policie
EU	Evropská unie
GDPR	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)
NCBK	Národní centrum kybernetické bezpečnosti
OÚ	Osobní údaje
SO ORP	Správní obvod obce s rozšířenou působností
SÚ	Subjekt údajů
IS	Informační systém
ICT	Informační a komunikační technologie
GIS	Geografický informační systém
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů
ZZOÚ	zákon č. 110/2019 Sb., o zpracování osobních údajů
VŘ	Výběrové řízení
Pojmy	
Osobní údaj	Veškeré informace o identifikovaném nebo identifikovatelném Subjektu údajů. Identifikovatelným Subjektem údajů je fyzická osoba,

(OÚ)	kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Jedná se o demonstrativní, a nikoliv úplný výčet.
Zvláštní kategorie osobních údajů **Citlivý osobní údaj (dále jen „COÚ“)**	Zvláštní kategorie osobních údajů jsou osobní údaje, které vypovídají, například o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech. Dále mezi osobní údaje patří genetické údaje nebo biometrické údaje jedinečně identifikující Subjekt údajů a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci Subjektu údajů; dále jen „zvláštní osobní údaje“ případně také jen „citlivé osobní údaje“
Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují a která je na základě těchto údajů identifikovatelná; může se jednat o zaměstnance, klienta/uživatele/pacienta, návštěvníka objektu, jiných osob atp.
Zpracování osobních údajů	Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které je prováděno pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, likvidace nebo zničení.
Správce	Každý subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Zpracováním osobních údajů může Správce zmocnit nebo pověřit Zpracovatele, pokud zvláštní zákon nestanoví jinak.
Zpracovatel	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro Správce.
Třetí osoba	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není Subjektem údajů, Správcem, Zpracovatelem ani osobou přímo podléhající Správci nebo Zpracovateli, jenž je oprávněna ke zpracování osobních údajů.
Princip „Need to know“	Objektivní a důvodná potřeba na straně oprávněné osoby seznámit se s osobním údajem za účelem plnění pracovních povinností či jiných povinností nebo oprávněných zájmů.
Automatizované zpracování osobních údajů	Operace uskutečňované zcela nebo zčásti pomocí automatizovaných postupů, zahrnuje operace typu: ukládání osobních údajů na nosiče informací, provádění logických a/nebo aritmetických operací s těmito osobními údaji, jejich změna, likvidace, vyhledávání nebo rozšiřování.

	Na základě této definice pak lze dospět k závěru, že proces profilování ve smyslu nařízení nemusí být zcela automatizovaný, ale že může být zapojen i lidský faktor.

2. ZÁVĚRY AUDITU

Na základě dohody bylo v rámci projektu **Koncepce města – pasporty – strategie - KOMPAS pro Uherský Brod, reg. č. CZ.03.4.74/0.0/0.0/16_058/0007427, Strategie ochrany osobních údajů ve veřejné správě,** uskutečněno nezávislé ověření shody současného nastavení a fungování procesů a bezpečnostních opatření ve městě Uherský Brod, včetně jeho Městské policie, s požadavky stanovenými GDPR a na ni navazující národní legislativou. Audit prověřil 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 a nastavení a fungování technických opatření,
- nastavení a fungování technických opatření.

Dokument se zpracován tak, aby byl v souladu s doporučeními ze strany ministerstva vnitra ČR.

Podrobná metodika realizace auditu tvoří Přílohu č. 2 tohoto dokumentu.

V době zahájení auditu byl platný zákon č. 101/2000 Sb. o ochraně osobních údajů. Tento byl zrušen a nahrazen tzv. „Adaptačním zákonem“ č. 110/ 2019 Sb., o zpracování osobních údajů. Veškerá zjištění byla posuzována dle současné platné legislativy.

Zjištění a neshody, které byly v průběhu auditu opraveny či uvedeny do odpovídajícího stavu, nejsou v této zprávě zmíněny.

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

4. MĚSTO UHERSKÝ BROD

Správní obvod obce s rozšířenou působností Uherský Brod je jedním ze 13 správních obvodů Zlínského kraje. Leží v jižní části kraje, na jihozápadě sousedí s Jihomoravským krajem a na jihu a východě pak se Slovenskou republikou. Uherský Brod je obcí s rozšířenou působností (tzv. obcí III. stupně), s čímž je také spojené zpracovávání většího množství OÚ. Do územní působnosti SO ORP Uherský Brod spadá 30 obcí, z nichž pouze Uherský Brod a Bojkovice mají statut města. K 1. 1. 2018 v obcích správního obvodu žilo 52 294 obyvatel. Městský úřad má počet zaměstnanců v rozmezí od 100–199.

Uherský Brod má v souladu se zák. č. 128/2000 Sb., o obcích (obecní zřízení) statut města. Nejvyšším orgánem Města ve věcech samostatné působnosti je Zastupitelstvo města Uherský Brod (dále jen "Zastupitelstvo města"). Výkonným orgánem města je Rada města Uherský Brod (dále jen "Rada města").

Zastupitelstvo města má v současnosti 27 členů a Rada města 9 členů. Zastupitelstvem města byl pro stávající volební období zvolen starosta, jako člen Zastupitelstva města uvolněný, první místostarosta, jako člen Zastupitelstva města neuvolněný, druhý místostarosta, jako člen Zastupitelstva města uvolněný, určený člen Rady města, jako člen Zastupitelstva města uvolněný. Zastupitelstvem je zvolena rada města, starosta města a dva místostarostové. Dalším orgánem města je Městský úřad Uherský Brod a Městská policie Uherský Brod.

Zastupitelstvo města má v současnosti 6 výborů, z toho 2 osadní výbory:

- Výbor finanční
- Výbor kontrolní
- Osadní výbor pro místní část Havřice
- Osadní výbor pro místní části Těšov – Újezdec
- Výbor pro strategický rozvoj
- Výbor pro životní prostředí

Rada města má dále 10 komisí:

- Komise pro cestovní ruch
- Komise bytová
- Komise pro bezpečnost a prevenci kriminality
- Komise pro školství
- Komise pro informatiku a Smart city

- Komise stavební a územního plánování
- Komise kulturní
- Komise dopravní
- Komise pro regeneraci a architekturu města
- Komise sportovní

Městský úřad Uherský Brod se organizačně rozděluje na:

- Odbor kanceláře tajemníka;
- Odbor správní;
- Odbor stavebního úřadu;
- Odbor finanční;
- Odbor životního prostředí;
- Odbor majetkoprávní;
- Odbor školství, kultury a sportu;
- Odbor sociálních věcí;
- Odbor rozvoje města;
- Odbor obecní živnostenský úřad.

Město Uherský Brod je zřizovatelem těchto příspěvkových organizací:

- TSUB, příspěvková organizace;
- CPA Delfín, příspěvková organizace;
- Dům dětí a mládeže Uherský Brod a Zařízení pro další vzdělávání pedagogických pracovníků, příspěvková organizace;
- Dům kultury Uherský Brod - příspěvková organizace;
    - Hvězdárna Domu kultury;
    - Knihovna Františka Kožíka;
    - Kino Máj Uherský Brod
- SOCIÁLNÍ SLUŽBY UHERSKÝ BROD, příspěvková organizace;
- Mateřské školy:
    - Mateřská škola Mariánské náměstí;
    - Mateřská škola Obchodní;
    - Mateřská škola Olšava;

- Mateřská škola Prim. Hájka;
- Mateřská škola Svatopluka Čecha;
- Základní škola a Mateřská škola Havřice;
- Mateřská škola Těšov;
- Základní škola a Mateřská škola Újezdec;

- Základní školy:
  - Základní škola Mariánské náměstí;
  - Základní škola Pod Vinohrady;
  - Základní škola Na Výsluní;
  - Základní škola a Mateřská škola Havřice;
  - Základní škola a Mateřská škola Újezdec.

Dále je Město zřizovatelem organizačních složek Jednotek sboru dobrovolných hasičů města Uherský Brod:

- Jednotka sboru dobrovolných hasičů Uherský Brod;
- Jednotka sboru dobrovolných hasičů Uherský Brod - Těšov;
- Jednotka sboru dobrovolných hasičů Uherský Brod - Havřice.

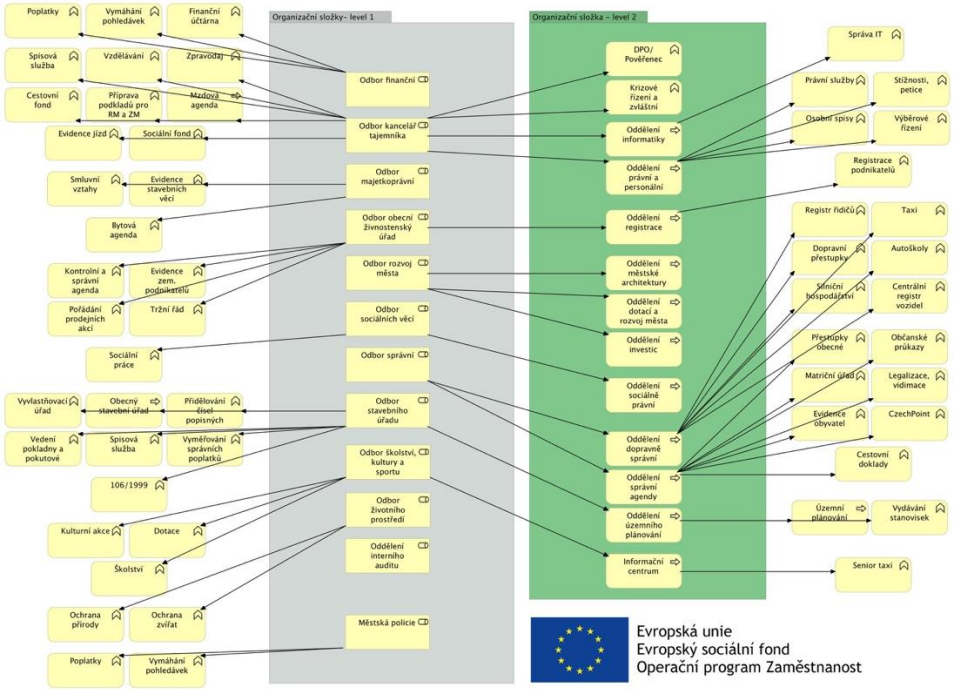
4.1 Identifikované oblasti zpracování osobních údajů

Město zpracovává osobní údaje v těchto identifikovaných oblastech (kompletní výčet je součástí procesních karet):

- evidence obyvatel,
- registr řidičů,
- zajišťování voleb,
- zabezpečování ochrany veřejného pořádku,
- při jednáních vedení obce/zastupitelů a v návazných zápisech či usneseních,
- sjednávání a uzavírání smluvních ujednání,
- správa a výběr správních/místních poplatků,
- správa majetku,
- ochrana životního prostředí,
- územní plánování,
- pořádání prodejních akcí,
- vnitřní kontrola,

- rozvoj města,
- zajišťování kulturního života obce včetně vítání občánků, evidence jubileí apod.,
- vedení kroniky,
- zdokumentování, informování o životě v obci, a to i za pomoci fotografických a jiných médií případně včetně místního časopisu,
- zajišťování vidimace a legalizace,
- zajištění personálních činností, mezd a vedení účetnictví,
- zajišťování sociálních služeb
- zřizovatel dalších příspěvkových organizací,
- zřizovatel městských společností,
- dotace,
- bytový fond,
- senior taxi,
- vydávání Brodského zpravodaje,
- informační centrum.

Mapa procesů v MěU Uherský Brod



Registrační číslo CZ.03.4.74/0.0/0.0/16_058/0007427

V souvislosti se zpracováním osobních údajů vystupuje město jako správce i zpracovatel osobních údajů.

4.2 Normy vztahující se k oblastem zpracování osobních údajů

4.2.1 Město Uherský Brod

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

- 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. 128/2000 Sb., o obcích,
- zákon č. 129/2000 Sb., o krajích,
- zákon č. 110/2019 Sb., o zpracování osobních údajů,
- 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. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- 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 (stavební zákon),
- 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,
- 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.

V souvislosti se zpracováním osobních údajů město Uherský Brod vydává obecně závazné vyhlášky, na základě zmocnění v čl. 104 ústavního zákona č. 1/1993 Sb., Ústava České republiky.

4.2.2 Městská policie Uherský Brod

Zpracování osobních údajů se v identifikovaných oblastech řídí především následujícími předpisy (výčet legislativy není kompletní):

- Zákon č. 89/2012 Sb., občanský zákoník,
- Zákon č. 553/1991 Sb., o obecní policii (včetně předpisu č. 311/2002 Sb., kterým se mění zákon o obecní policii),
- Vyhláška č. 418/2008 Sb., kterou se provádí zákon o obecní policii,
- Zákon č.110/2019 Sb., o zpracování osobních údajů,
- Zákon č. 328/1999 Sb., o občanských průkazech,
- OZV č. 1/1995, o zřízení, postavení a hlavních úkolech městské policie ve znění OZV č. 6/2005, kterou se mění a doplňuje obecně závazná vyhláška č. 1/1995 o zřízení, postavení a hlavních úkolech městské policie.

4.2.3 Příspěvkové organizace

Příspěvkové organizace nebyly předmětem zkoumání v rámci projektu „KOMPAS“.

4.2.4 Městské společnosti s ručením omezeným

Městské společnosti nebyly předmětem zkoumání v rámci projektu „KOMPAS“.

4.3 Rizikové zpracování osobních údajů

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) předpokládá v některých případech vypracování posouzení vlivu na ochranu osobních údajů. Takové posouzení je nutné v případech, kdy zpracování osobních údajů má za následek vznik vysokého rizika pro práva a svobody fyzických osob, a to s přihlédnutím k povaze, rozsahu, kontextu, účelům zpracování a využitím nových technologií. Samo nařízení poskytuje v článku 35 odst. 1 a odst. 3 několik vodítek k určení úrovně vysokého rizika pro práva a svobody fyzických osob při zpracování osobních údajů. Zdůrazněna jsou zejména taková zpracování osobních údajů, při nichž dochází:

(i) k systematickému a rozsáhlému vyhodnocování osobních aspektů, založenému na automatizovaném zpracování (včetně profilování), kdy dochází k rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají podobný závažný dopad;

(ii) k rozsáhlému zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků ve věcech trestních;

(iii) nebo dochází k rozsáhlému systematickému monitorování veřejných prostranství.

Uvedený text je však poměrně obecný a ve většině případů neumožňuje jednoznačné zařazení konkrétního zpracování osobních údajů. Proto je nutné další upřesňování parametrů, které se pokusila provést WP29 v rámci dokumentu WP248 („Guidelines on Data Protection Impact Assessment (DPIA) and determining wheter processing is „likely to result in a high risk“) for purposes of regulation 2016/679“, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137), určeného zejména pro správce, zpracovatele a dozorové orgány. Text nastiňuje podrobněji přístup k řešení této problematiky a jsou v něm naznačena podrobnější východiska pro určení rizikovosti (například k definici pojmů rozsáhlé zpracování), ale rovněž bez podrobnějších hodnot kritérií.

V rámci dokumentu je stanoveno 9 obecných kritérií pro stanovení vysoké rizikovosti zpracování osobních údajů:

1. provádí se ohodnocení nebo hodnocení bonity fyzických osob, včetně profilování a předpovědi;
2. provádí se automatické rozhodování s právním nebo obdobným významným účinkem;
3. provádí se systematické monitorování, včetně monitorování veřejně přístupných prostor;
4. provádí se zpracování citlivých údajů;
5. provádí se zpracování velkého rozsahu;
6. provádí se kombinace nebo propojování dat různých zpracování;
7. provádí se zpracování údajů týkající se zranitelných subjektů údajů;
8. dochází k inovativnímu využití nebo aplikaci technologických nebo organizačních řešení;

9. provádí se zpracování s obtížně uplatnitelnými právy subjektů údajů - pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy.

Lze předpokládat, že budou existovat zpracování osobních údajů, která by na základě analýzy mohla být zařazena do skupiny „zpracování s vysokým rizikem pro práva a svobody subjektů údajů“, nicméně na základě empirických poznatků a případně i snahy po minimálním administrativním zatížení některých správců dochází evropské nebo národní orgány k závěru, že zpracování posouzení vlivu na ochranu osobních údajů v těchto případech není třeba provádět. O takových výjimkách (například čl. 35 odst. 10 a recitál bod 91 GDPR) tedy rozhodují i jiné faktory, které se nedají kritérii jednoduše vyjádřit. Jednou z těchto výjimek je zpracování (operace zpracování), která se řídí právními předpisy (viz čl. 35 odst. 10 GDPR) a na která bylo posouzení vlivu na ochranu osobních údajů provedeno jako součást obecného posouzení (pokud posouzení splňuje požadavky na hodnocení vlivu na ochranu osobních údajů dle GDPR) v souvislosti s přijetím právního předpisu. Správce to však v žádném případě nezbavuje povinnosti osobní údaje přiměřeně zabezpečit.

4.4 Zdroje informací

V průběhu auditu byly poskytnuty k nahlédnutí vybrané dokumenty, dále bylo auditorům umožněno nahlédnout do kanceláří a zjistit, jak jsou dokumenty obsahující osobní údaje fyzických osob v listinné podobě uloženy a zabezpečeny.

Auditoři provedli rozhovory s následujícími osobami odpovědnými za činnosti související se zpracováním osobních údajů:

Jméno a příjmení	Funkce/agenda
	Tajemník
	Oddělení právní a personální
	Oddělení právní a personální
	Oddělení informatiky
	Krizové řízení a zvláštní úkoly
	Odbor správní
	Oddělení správní agendy
	Oddělení dopravně správní činnosti a agendy
	Odbor stavebního úřadu

	Odbor stavebního úřadu
	Oddělení územního plánování
	Odbor finanční
	Odbor majetkoprávní
	Odbor majetkoprávní
	Odbor školství, kultury a sportu
	Městské informační centrum
	Odbor sociálních věcí
	Oddělení sociálně právní ochrany dětí
	Odbor rozvoje města
	Oddělení dotací a rozvoje města
	Oddělení městské architektury
	Oddělení investic
	Odbor obecní živnostenský úřad
	Oddělení registrace
	Oddělení interního auditu
	Městská policie

4.5 Správa osobních údajů

4.5.1 Zdroje osobních údajů

Město shromažďuje a zpracovává osobní údaje fyzických osob, které mají zájem o jeho služby či spadají pod jeho působnost. Údaje jsou získávané 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.

4.5.2 Zpracování osobních údajů

Správce zpracovává osobní údaje a další informace týkající se subjektů osobních údajů v rámci samostatné a přenesené působnosti. Většina osobních údajů je zpracovávána na základě povinností, uložených zvláštními zákony. Na taková zpracování osobních údajů o subjektech údajů se nevztahuje povinnost získat souhlas těchto osob. Pokud jsou některé osobní údaje zpracovávány mimo zákonnou povinnost, pak taková zpracování podléhají souhlasu subjektu údajů. Město zpracovává OÚ na základě souhlasu pouze v případě zveřejňování osobních údajů např. v Brodském zpravodaji.

4.5.3 Umístění osobních údajů

Osobní údaje jsou uchovávány buď v listinné podobě v jednotlivých odborech úřadu, nebo v elektronické podobě v příslušných aplikacích Města a státní správy (především IS EZOP VITA, Helios). Obvykle jsou osobní data zpracovávána také za pomoci běžného kancelářského softwaru. Osobní údaje mohou být také obsahem e-mailové komunikace v rámci úřadu a dále mezi MÚUB a volenými členy komisí a výborů (dle zákona o obcích).

Fyzicky jsou elektronická data umístěna v počítačové síti úřadu. Dále MÚUB pracuje s osobními údaji v rámci systému Czech Point. Počítače jsou zpravidla chráněny heslem, přístupy do IS (EZOP, VITA, Helios), popř. systému Czech Point jsou možné prostřednictvím uživatelských účtů s přidělenými uživatelskými právy či prostřednictvím certifikátů. Uživatelské účty jsou chráněny přístupovými hesly. Na PC je instalován pouze legálně pořízený software, je využíván antivir.

Ukládání dat probíhá denně na servery a dále zálohování na další server, data jsou šifrována.

Životní cyklus osobních údajů

Po celou dobu životního cyklu zpracovávaných osobních údajů je potřeba si nepřetržitě pokládat otázku „kdy a jak dlouho“. Jedním z principů, které GDPR prosazuje, je totiž přesnost a aktuálnost zpracovávaných osobních údajů. Proto je potřeba, aby se v průběhu celého procesu dbalo na to, že jsou zpracovávány jen ty údaje, které jsou nezbytně nutné k danému účelu a hlavně, že jsou aktuální.

Tento proces vás bude nutit k tomu, že nepotřebná data musíte vymazat, pokud jsou zpracovávána například na základě souhlasu osoby, která svůj souhlas odvolala. Nezapomeňte, že tato data musí být vymazána ve všech úložištích včetně těch záložních.

Ve spisovém a skartačnímu řádu musí být stanovena doba, po kterou s osobními údaji disponujete, a tu si umět náležitě obhájit. Rozhodně nebude stačit prohlášení, že zpracováváte údaje po dobu nezbytně nutnou. Životní cyklus dat musí mít jasné ohraničení začátku a konce.

4.6 Zajištění personálních činností ve vztahu k zaměstnancům města

4.6.1 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).

4.6.2 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 v mzdovém software a jsou také součástí kancelářského softwaru včetně e-mailové komunikace. Přístup k osobním údajům zaměstnanců vedeným elektronicky je možný pouze pro oprávněné osoby (personální oddělení) za pomoci přístupového hesla (přístup do příslušných IS).

4.6.3 Smlouvy a dohody

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. Je tedy třeba zajistit úplnost znění povinnosti mlčenlivosti všech zaměstnanců a ne pouze úředníků.

4.6.4 Výběrové řízení

Součástí výběru budoucích zaměstnanců je hodnocení informací obsažených v životopisech, které Město obdrželo od uchazečů o zaměstnání. Ve zveřejněných výběrových řízení na příslušné pracovní pozice se po uchazečích nepožaduje souhlas se zpracováním osobních údajů, a to ani po skončení výběrového řízení. Tento přístup je v souladu s GDPR (jedná se o jednání za účelem uzavření smlouvy).

4.6.5 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 starosty, místostarosty, zastupitelů a tajemníka 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.

4.6.6 Zpracování po ukončení pracovněprávního vztahu

Po ukončení pracovněprávního vztahu nejsou písemnosti tvořící osobní spis zaměstnance protříděny a jsou dále uchovávány. Bylo by vhodné aktualizovat vnitřní předpis č. 01/2006 Spisový a skartační řád, tak aby jasně stanovoval, jaké dokumenty je potřeba dále uchovávat v osobním spise.

4.6.7 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, kdy jsou zpracovávány OÚ zvláštní kategorie, lze považovat informace o zdravotním stavu zaměstnanců (vstupní a 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 diagnóza). Zprávy jsou součástí osobní složky zaměstnance.

4.7 Zabezpečení zpracovávaných údajů

Data vedená v elektronické podobě jsou poměrně dostatečně zabezpečena, přístup do PC je vždy chráněn heslem. Díky tomu, že nikdo z běžných uživatelů není veden jako administrátor, je zabráněno neoprávněnému přístupu k diskům, a tak také k osobním datům, které by bylo možné zneužít.

Je také potřeba neponechávat PC bez dozoru, při opuštění stanice se od svého uživatelského účtu odhlásit či mít při určité době nečinnosti nastaveno přepnutí na spořič obrazovky s nutností opakovaného přihlášení apod. Dále je třeba nenechávat dokumenty obsahující osobní údaje volně na stolech zaměstnanců (byť při krátkodobém přerušení práce a opuštění kanceláře, tím spíše pokud je případně kancelář sdílena s dalším zaměstnancem).

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 podmínkách 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.

Zajištění serveroven odpovídalo v době auditu bezpečnostním standardům.

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.

4.8 Souhrn klíčových zjištění auditu

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

5. PODROBNÝ POPIS ZJIŠTĚNÍ A 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.

5.1 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.

5.2 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.

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).

5.3 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 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.

5.4 Evidence uchovávaných/zpracovávaných osobních údajů včetně umístění

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 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.

5.5 Informační povinnost o zpracování osobních údajů

Legislativní rámec:

Čl. 12 odst. 1 GDPR 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 uvést veškerá sdělení podle čl. 15 až 22 a 34 GDPR. 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.

5.6 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 GDPR 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 GDPR.

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.

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.

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.

5.7 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 službě musí být stanovené archivační a skartační lhůty.

5.8 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 Evropské 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 čl. 28 odst. 3 GDPR. 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.

5.9 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).

5.10 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.

5.11 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.

5.12 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.

5.13 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.

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.

5.14 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.

6. MĚSTSKÁ POLICIE

Městská policie zabezpečuje místní záležitosti v oblasti veřejného pořádku v působnosti města. Režim služeb je 24hodinový.

Městská policie zpracovává pouze omezený rozsah osobních údajů (především v souladu s ustanoveními § 11a zákona č. 553/1991 Sb., o obecní policii). Městská policie je oprávněna především získávat osobní údaje z příslušných IS (IS Policie, registr obyvatel, rejstřík trestů) či samostatně zjišťovat a ověřovat následující údaje:

- příjmení,
- jméno, popřípadě jména,
- adresa místa pobytu, případně též adresa, na kterou mají být doručovány písemnosti podle zvláštního právního předpisu,
- datum, místo a okres narození,
- rodné číslo,
- státní občanství, popřípadě více státních občanství,
- adresa místa trvalého pobytu, případně též adresa, na kterou mají být doručovány písemnosti podle zvláštního právního předpisu,
- omezení svéprávnosti + jméno, příjmení a rodné číslo opatrovníka,
- jméno, příjmení a rodné číslo otce, matky, popřípadě jiného zákonného zástupce,
- zákaz pobytu, místo zákazu pobytu a doba jeho trvání,
- správní nebo soudní vyhoštění a doba, po kterou není cizinci umožněn vstup na území České republiky.

Všechny uvedené údaje jsou získávány prostřednictvím přístupu do příslušných IS a na základě ustanovení zákona, tedy zákonně, není potřeba pro ně získávat jakýkoliv souhlas.

Správu IT si zajišťují sami. Ve Městě je pro sledování dopravní situace i zajištění bezpečnosti občanů a majetku instalován kamerový systém. Celkem je nainstalování 22 kamer z toho 7 je stacionárních, ostatní se mohou natáčet. Servis zajišťuje externí firma SKS s.r.o. Blansko.

S MěÚ dochází ke komunikaci prostřednictvím svodek událostí a dále především osobně/ústně, e-maily jsou využívány v omezené míře, a pokud ano, neobsahují osobní údaje fyzických osob, není tedy třeba, aby byly šifrovány.

Personální agendu pro MP zajišťuje MěÚ, související osobní údaje a jejich zpracování tak leží mimo působnost MP. MP má pouze část osobních spisů kvůli povinnostem ze zákona o obecní policii (osvědčení o odborné způsobilosti).

6.1 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 Evropské 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 z čl. 28 odst. 3 GDPR. 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.

6.2 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.

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.

7. CELKOVÉ HODNOCENÍ

Na základě provedeného auditu, tj. osobních návštěv Města (prohlídka všech prostor a budov MěÚ, rozhovory s vybranými zaměstnanci apod.), prostudování předložených materiálů v elektronické i listinné podobě, kontrole webových stránek a profilů na sociálních sítích Města a dostupných veřejných zdrojů je možné konstatovat, že

město Uherský Brod splňuje soulad s požadavky GDPR.

Celková organizace činností souvisejících s ochranou osobních údajů ve Městě, vedoucí jednotlivých odborů, osoba Pověřence a deklarovaná podpora vedení, dávají záruku, že tento soulad zůstane zachován i nadále a Město bude schopné reagovat na změny legislativních podmínek souvisejících s ochranou osobních údajů, včetně připravované evropské směrnice ePrivacy.

Právě vhodný výběr osoby Pověřence se ukazuje jako klíčový faktor úspěšného zajištění souladu s požadavky GDPR. Druhým faktorem je správné zařazení Pověřence do organizační struktury a celková podpora vedení Města.

8. PŘÍLOHY

Příloha č. 1: Zdroje informací

Příloha č. 2: Metodika auditu

Příloha č. 3: Kontextové informace k ochraně osobních údajů

Příloha č. 1: Zdroje informací

Hlavním zdrojem informací byly obdržené písemné podklady a rozhovory se zaměstnanci.

Audit byl proveden na základě přezkoumání obdržených písemných podkladů, dále v součinnosti s DPO a dle potřeby také byli přizváni další odpovědní zaměstnanci, kteří formou rozhovorů poskytli auditorům doplňující informace.

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

- Interní řídící dokumentace MěU,
- Formuláře a protokoly používané v MěU,
- Dotazy na zpracování osobních MěU.

Příloha č. 2: 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 zpracování 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 zpracování 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,
- 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 v obecném nařízení 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

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 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

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

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

Příloha č.3: 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 byla od 25. května 2018 nahrazena obecným nařízením o ochraně osobních údajů (GDPR).

Obecným právním předpisem ochrany osobních údajů v ČR bylo v době zahájení auditu obecné nařízením GDPR a zákon č. 110/2000 Sb., o zpracování osobních údajů a zákon č. 111/2019 Sb., o změně některých zákonů.