Analýza připravenosti společnosti k souladu s nařízením EU 2016/679 o ochraně osobních údajů . (GDPR)

Auditovaný:
Město Nové Sedlo
se sídlem: Masarykova 502, 357 34 Nové Sedlo
zastoupený: Ing. Věra Baumanová, starostka
IČ: 00259527
DIČ: CZ00259527.
Kontaktní osoba: Ing. Karel Tetur
Tel.: 737 202 907
e-mail: tajemnik@mestonovesedlo.cz

Zhotovitel:
VARiKO s.r.o.

Stav zpracování ke dni:
21.5.2018

Obsah

PŘÍLOHY

1. Sběrné formuláře k jednotlivým agendám
2. Vyhodnocení souladu s GDPR u jednotlivých agend
3. Doporučená opatření u jednotlivých agend
4. Doporučená opatření společná
5. Seznam zákonů
6. Základní školící materiál GDPR
7. Prezenční listina

1. Identifikační údaje.

Město Nové Sedlo

se sídlem: Masarykova 502, 357 34 Nové Sedlo

zastoupený: Ing. Věra Baumanová, starostka

IČ: 00259527

DIČ: CZ00259527.

Kontaktní osoba: Ing. Karel Tetur

Tel.: 737 202 907

e-mail: tajemnik@mestonovesedlo.cz

1.1. Profil auditované společnosti.

Poprvé je Nové Sedlo uváděno v písemných pramenech roku 1397. V polovině 19. století se stává samostatnou obcí. Roku 1899 bylo povýšeno na městys a byl mu udělen znak. V téže době nastává rozvoj obce. V současné době je Nové Sedlo klasifikováno jako město s cca 2600 obyvateli.

Město Nové Sedlo je zřizovatelem :

- TJ Baník Union Nové Sedlo
- Městské knihovny
- Základní školy
- Mateřské školy
- MAS Sokolovsko
- Mikroregion Sokolov-východ

(Výše uvedené organizace nejsou předmětem analýzy)

2. Úvodní slovo

Obecné nařízení Evropského parlamentu a Rady EU (EU 2016/679) ze dne 27.4.2016, **označované jako GDPR (General Data Protection Regulation), nebo jen Obecné nařízení, představuje právní rámec ochrany osobních údajů platný na celém území Evropské unie a** vstoupí v platnost 25.5.2018
Obecné nařízení se dotkne všech subjektů zpracovávajících osobní údaje, a to napříč odvětvími. Nahrazuje předchozí právní úpravu - **Směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995.**

Obecné nařízení klade důraz na vymahatelnost práv fyzických osob a povinnosti správců a zpracovatelů osobních údajů fyzických osob. Pro všechny správce a zpracovatele osobních údajů **je důležité, aby měli všechny své systémy připravené na naplňování práv subjektů údajů (fyzických osob) a své činnosti (agendy) vykonávané s osobními údaji fyzických osob byly v souladu s obecným nařízením EU (GDPR). Jinak se vystavují značnému riziku sankcí, které můžou být pro ně bolestivé.**

Tento materiál si klade za cíl analyzovat stávající stav zpracování osobních údajů u auditovaného subjektu a posoudit jej z hlediska jeho připravenosti na změny, které čekají všechny subjekty pracující s osobními údaji v roli správce, nebo zpracovatele, v souvislosti s účinností Obecného nařízením o ochraně osobních údajů (EU 2016/679), které vstoupí v platnost 25.5.2018. Tato fáze je prvním důležitým krokem v celkovém procesu nastavení všech činností zpracování osobních údajů tak, aby byly v souladu ze základními požadavky a principy ochrany osobních údajů, tak jak je definuje Obecné nařízení .

2.1. Cíle analýzy

Analýza si kladla za cíl zejména:

- zjištění stávajícího stavu zpracování osobních údajů
- proškolit zpracovatele osobních údajů ze základní problematicky ochrany a principů zpracování dle Obecného nařízení
- identifikovat jednotlivé agendy zpracování
- monitorovat rozsah a formy zpracování osobních údajů u jednotlivých agend
- identifikace kategorií osobních údajů u jednotlivých agend
- vyhodnotit zákonnost zpracování
- zjištění stavu dokumentace a nastavení veškerých procesů a činností v celém životním cyklu zpracování osobních údajů
- identifikace pravidel a opatření zajišťujících naplňování práv subjektů údajů
- identifikace prostředí (systémů), ve kterých dochází ke zpracování osobních údajů a způsob jejich ochrany.
- identifikace nesouladu s nařízením GDPR
- návrh opatření

2.2. Obsah a průběh analýzy

Prvním krokem k dosažení výše uvedených cílů bylo **zjištění stávajícího stavu** zpracování osobních údajů. Sběr dat probíhal za účasti a blízké spolupráce s jednotlivými zaměstnanci organizace, kteří s danou agendou bezprostředně pracují v praxi.

Pro dobré pochopení problematiky, byl sběr dat zahájen **vstupním proškolením** jednotlivých zpracovatelů agend ze základní problematiky ochrany osobních údajů s cílem vysvětlit základní principy Obecného nařízení, důvody, strukturu sběrných formulářů a vzájemný vztah a návaznost jednotlivých položek v samotných formulářích. Prezentace přednesená v rámci školení je součástí tohoto materiálu jako příloha č. 6. Součástí proškolení byl ve shodě vymezen pojem „agenda" (ucelený okruh/množina osobních údajů zpracovávaných za určitým konkrétním účelem) jako základní prvek sledování stavu zpracování osobních údajů a **identifikovány jednotlivé agendy** zpracování u auditované organizace (viz dále kapitola *„Identifikované agendy zpracování osobních údajů"*….).

Samotný sběr dat byl prováděn formou strukturovaných sběrných formulářů, které obsahovali sedmnáct základních položek vypracovávaných **pro každou identifikovanou agendu zvlášť**. V průběhu sběru proběhlo několik konzultačních schůzek s jednotlivými zpracovateli agend s cílem upřesnění údajů a získání ucelené představy aktuálního stavu zpracování osobních údajů a to zejména identifikace:

- činností zpracování osobních údajů
- uživatelů, zpracovatelů, příjemců osobních údajů
- osobních údajů, kategorie osobních údajů
- zdroje osobních údajů, kategorie subjektů údajů
- technických a organizačních opatření ochrany osobních údajů
- stávající dokumentace související se zpracováním osobních údajů
- vyhodnocení dodržování principů ochrany zpracování osobních údajů

Tato fáze byla i vzhledem k objektivním podmínkám (zejména pracovní vytížení spolupracujících zaměstnanců) časově nejnáročnější. Zpracované sběrné formulář popisující stávající stav u jednotlivých agend byly následně týmem auditorů podrobeny analýze z hlediska připravenosti a souladu s principy Obecného nařízení.

Za účelem přehledného vyhodnocení stavu jednotlivých agend zpracování osobních údajů, byl vypracován hodnotící formulář pro každou agendu samostatně, který identifikuje jednotlivé body shody, případně neshody s principy Obecného nařízení. Na základě tohoto formuláře následně auditoři, ve spolupráci s garanty jednotlivých agend, vypracovali návrhy doporučení pro řešení jednotlivých neshod, včetně návrhu harmonogramu pro přijmutí jednotlivých opatření. (viz podrobněji kapitola „Doporučená opatření")

3. Použité základní pojmy a zkratky

- **Seznam pojmů**

Osobní údaje - veškeré *údaje o identifikované, nebo identifikovatelné osob.*

Osobní údaje zvláštní kategorie - *údaje o zdravotním stavu, informace o rasovém, národnostním, náboženském a etnickém původu, genetické a biometrické údaje schopné identifikovat konkrétní osobu, rovněž politické názory, nebo členství v odborech, údaje o sexuálním životě a orientaci, záznamy o sociální situaci…*

Subjekt údajů - *fyzická osoba, u které dochází ke zpracování jejich osobních údajů.*

Správce – *subjekt (právnická, nebo fyzická osoba) určující účel a prostředky zpracování dat.*

Zpracovatel - subjekt *(právnická, nebo fyzická osoba)* zpracovávající osobní údaje pro správce, vykonávající určité činnosti s osobními údaji dle pověření správce

Příjemce – *fyzická, nebo právnická osoba (externí subjekt), kterému jsou osobní údaje poskytnuty, na základě určitého mandátu. Orgány veřejné moci, které mohou získávat osobní údaje na základě zvláštního šetření, se za příjemce nepovažují.*

Dozorový úřad – *nezávislý orgán veřejné moci, zřízený členským státem EU (v ČR Úřad pro ochranu osobních údajů)*

Zpracování osobních údajů - *všechny činnosti, které jsou provedené nad osobními údaji Subjektu údajů. (pořizování, ukládání, třídění, vyhledávání, nahlížení, kombinování, výmaz, nahrávání, prezentování…)*

Porušení zabezpečení osobních údajů – *porušení, které vede k náhodnému, nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí (zpřístupnění) osobních údajů*

Práva Subjektu údajů:
…na přístup - *právo získat od Správce potvrzení, zda o něm zpracovává osobní údaje a pokud ano, má právo získat přístup k těmto osobním údajům a k podrobnostem o zpracování.*
…na přenositelnost - *právo získat své osobní údaje ve strojově zpracovatelném formátu.*
…podat námitku – *právo podat námitku proti zpracování osobních údajů (při zpracování údajů založeném na oprávněném zájmu, případně proti porušení dalších zásad zpracování).*
…na omezení zpracování – *právo zažádat o omezení zpracování do doby vyřešení námitky.*
…na opravu – *právo na bezodkladnou opravu nepřesných údajů.*
…na výmaz – *právo na vymazání dat když jsou data zpracovávána protiprávně, když Subjekt údajů vznesl oprávněnou námitku.*
…na omezení automatizovaného rozhodování – *právo nebýt součástí výhradně automatizovaného rozhodování, profilování.*
(podrobněji v příloze č. 6.)

Základní principy zpracování osobních údajů:
…Účelové omezení - *pracování je možné provádět pouze pro daný účel.*
*…**Minimalizace** - osobní údaje zpracovávat pouze pro stanovený účel po nezbytně dlouhou (minimální) dobu a v nezbytně velkém (minimálním) rozsahu*
*…**Přesnost -** údaje musí být přesné, v případě potřeby pravidelně aktualizované.*
*…**Integrita, Důvěrnost -** ochrana dat vhodnými prostředky proti narušení integrity a důvěrnosti - zničení, zkreslení, poškození, protiprávnímu zneužití, neoprávněnému přístupu, zajištění dostupnosti a schopnosti obnovy.*
*…**Transparentnost -** informace o zpracování osobních údajů musí být komplexní, snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků.*
*…**Zákonnost -** Zpracování je zákonné, pokud existuje právní základ, dle kterého získává Správce mandát pro zpracování osobních údajů.*
(podrobněji v příloze č. 6.)

Základní povinnosti Správce:
…provádět záměrná a standardní opatření pro ochranu osobních údajů
…odpovědnost za výběr zpracovatele osobních údajů
…vést dokumentaci o činnostech zpracování osobních údajů
…provádět posuzování vlivu na ochranu osobních údajů, případně předchozí konzultaci
…ohlašovací povinnost při bezpečnostním incidentu
…naplňování práv Subjektu údajů
…jmenování pověřence pro ochranu osobních údajů
(podrobněji v příloze č. 6.)

- **Seznam zkratek**

GDPR - ***G**eneral **D**ata **P**rotection **R**egulation (nařízení Evropského parlamentu a Rady EU (EU 2016/679) ze dne 27.4.2016)*

DPO - ***D**ata **P**rotection **O**fficer (Pověřenec pro ochranu osobních údajů)*

ÚOOÚ – *Úřad pro ochranu osobních údajů – dozorový úřad pro dohled a naplňování zásad ochrany osobních údajů pro Českou republiku*

***MAC adresa** - "Fyzická adresa". Je to jedinečný identifikátor síťového zařízení - je to číslo, které zařízení dostane již při její výrobě.*

***IP adresa** -Adresa každého zařízení připojeného k počítačové síti používající Internet Protocol (IP).*

VPN - *Virtuální privátní (soukromá) počítačová síť*

BP *– Bezpečnostní politika*

Flash disk *– paměťové zařízení pro ukládání dat*

HW *– Fyzická část výpočetní techniky*

IT *– Informační technologie*

SW *– Programové vybavení výpočetní techniky*

UPS *– Nepřerušitelný zdroj energie*

Log *– Kontrolní auditní záznam*

IS *– Informační systém*

4. Identifikované agendy zpracování osobních údajů – mapování stávajícího stavu

Ve spolupráci se zástupci zadavatele (garanty jednotlivých agend) byly všechny identifikované agendy zpracování osobních údajů podrobeny prozkoumání metodou strukturovaných dotazů. Výsledkem tohoto šetření jsou data zpracované do přehledných tabulek pro každou agendu zvlášť.
V tabulce 1 níže, jsou uvedené sumární data. Podrobné informace, které byly následně předmětem vyhodnocení souladu, jsou součástí příloh. (*Příloha 1 - Sběrné formuláře k jednotlivým agendám*)

Město Nové Sedlo Tabulka č. 1

Seznam agend	ID agendy	Účel zpracování	Zpracovatel	Příjemci	Zdroj dat / Kategorie subjektů údajů	Kategorie osobních údajů	Forma zpracování	SW prostředí
BOZP	***01***	*Proškolování zaměstnanců v rámci bezpečnosti a ochrany zdraví při práci*	*není*	*Kontrolní orgány Inspektorát práce práce, Úřad práce, Policie, Krajské hygienická stanice, pojišťovny, OSSZ*	*zaměstnanci*	*osobní údaje*	*listinná*	*není*
Prezentační materiály města	***02***	*Účelem je dokumentace kulturních akcí v našem městě a přehled dění ve městě, místní rozhlas - informace občanům*	*není*	*není*	*účstníci akcí*	*osobní údaje + údaje zvláštní kategorie*	*listinné i digitální*	*cloud Google*
CZECHPOINT	***03***	*Služba občanům -vydávání ověř.výstupů z informač.systémů veřej.správy*	*není*	*není*	*žadatelé*	*osobní údaje*	*listinné i digitální*	*aplikace ministerstva vnitra*
Evidence klientů knihovny	***04***	*Účelem zpracování je evidence čtenářů*	*ChanGroup s.r.o. Lanius*	*není*	*Děti a studenti, zákonný zástupci žáků, zaměstnanci, obyvatelé*	*osobní údaje*	*listinné i digitální*	*SW Clavius*
Evidence obyvatel	***05***	*Účelem zpracování osobních údajů jsou činnosti v souvislosti s přenesenou působností evidence obyvatel*	*ChanGroup s.r.o. , TRIADA, s.r.o.*	*vlastníci nemovitosti, soudy, PČR, ORP, …*	*žadatelé*	*osobní údaje + údaje zvláštní kategorie*	*listinné i digitální*	*SW Munis*
Evidence zákazníků sběrného dvora	***06***	*Účelem zpracování je vedení záznamů o zakaznících, kteří přivezli odpad do sběrného dvora*	*INISOFT s.r.o.*	*není*	*obyvatelé*	*osobní údaje*	*listinné i digitální*	*SW EVI8*
Grantový systém města	***07***	*Vedení seznamu žadatelů o dotaci a veřejnoprávní smlouvy příjemců dotací*	*není*	*není*	*žadatelé*	*osobní údaje*	*listinné i digitální*	*Word, excel*

Poskytování informací dle zákona 106/1999 Sb.	**08**	Účelem zpracování je vedení záznamů poskytnutých informací podle zákona 106/1999 Sb., právní povinnost	není	není	obyvatele EU	osobní údaje	listinné i digitální	Word, excel
Kácení stromů	**09**	Evidence žádostí a vyřízení kácení stromů	PilsCom s. r.o., Changroup s.r.o.	Městský úřad Sokolov	žadatelé	osobní údaje	listinné i digitální	Word, excel
Matriční kniha manželství	**10**	Výkon státní správy na úseku matrik	není	Státní oblastní archiv Plzeň	fyzické osoby	osobní údaje	listinná	není
Matriční kniha narození	**11**	Výkon státní správy na úseku matrik	není	Státní oblastní archiv Plzeň	fyzické osoby	osobní údaje	listinná	není
Matriční kniha úmrtí	**12**	Výkon státní správy na úseku matrik	není	Státní oblastní archiv Plzeň	fyzické osoby	osobní údaje	listinná	není
Evidence místních polatků	**13**	Účelem zpracování je vedení evidence místních poplatků	Triada s.r.o.	není	žadatelé	osobní údaje	listinné i digitální	Munis
Kamerový systém	**14**	Účelem kamerového systému je ochrana majetku a osob	není	Police	občané	osobní údaje + údaje zvláštní kategorie	digitální	není
Příkazní řízení	**15**	Zpracování osobních údajů při evidenci a řešení přestupků	není	není	přestupci	osobní údaje	listinné i digitální	ISEMP SW
Veřejné opatrovnictví	**16**	Vedení údajů osob s omezenou svéprávností	není	soud	opatrovníci	osobní údaje + údaje zvláštní kategorie	listinná	Word
Rozhodování v matričních záležitostech	**17**	Výkon státní správy na úseku matrik	není	není	žadatelé	osobní údaje	listinné i digitální	Word, spis. Služba
Evidence zaměstnanců - spis	**18**	Personální evidence zaměstnanců úřadu	není	není	zaměstnanci	osobní údaje + údaje zvláštní kategorie	listinné i digitální	Word
Evidence zaměstnanců - mzdová agenda	**19**	Zpracování mezd stálých zaměstnanců i zaměstnanců zaměstnaných na dohody o pracovní činnosti a dohod o provedení práce	Ing. Jiří Matoušek	pojišťovny, OSSZ, Finanční úřad, Úřad práce, soudy	zaměstnanci	osobní údaje + údaje zvláštní kategorie	listinné i digitální	Tringl SW
Pokladna	**20**	Zpracování osobních údajů v souvislosti s evidencí výdeje a příjmu plateb v hotovosti	TRIÁDA s.r.o.	nikdo	zaměstnanci, klienti (vč. obyvatel města)	osobní údaje	listinné i digitální	Sw Munis

Posudky	**21**	Vypracovávání posudků na základě žádostí, spolupráce se soudy, PČR, OSPOD,…	nikdo	soudy, PČR, MÚ, KÚ, OSPOD, ostatní instituce	občané s TP v obci; občané, kteří na území obce žijí	osobní údaje	listinná	není
Povolení k umístění herního prostoru	**22**	Vydávání povolení k umístění herního prostoru	nikdo	ministerstvo, celní úřad	žadatelé	osobní údaje	listinné i digitální	modul MF
Pozemní komunikace a Územní plánování	**23**	Zpracovávání Rozhodnutí zvláštního užívání místní komunikace a na základě žádosti fyzické osoby (občana) i podněty na změny územního plánu	nikdo	MÚ Chodov, MÚ Sokolov, KÚKK	žadatelé	osobní údaje	listinné i digitální	Word
Pracovní úrazy	**24**	Účelem zpracování je vedení záznamů o pracovních úrazech a zpracovní podkladů pro přiznání pojistného plnění	nikdo	pojišťovny, Oblastní inspektorát prácePlzeň, OSSZ, policie	zaměstnanci	osobní údaje	listinná	Word
Přestupkové řízení	**25**	Přestupkové řízení - zákon č. 250/2016 Sb.	Changroup s.r o.	soudy, PČR, státní zastupitelství	přestupci	osobní údaje	listinné i digitální	Sw Vita
Prodej nemovitostí	**26**	Vedení evidence přehledu majetku	PilsCom s.r.o. , Advokátní kancelář JUDr. Erika Justová	katastrální úřad	fyzické osoby - klienti, kterým se stala matriční událost	osobní údaje	listinné i digitální	SW Athena
Pronájem bytů	**27**	Účelem zpracování je sepsání nájemní smlouvy, výpočtového listu pro měsíční platby a případné následné vymáhání dluhů u soudu.	Koncept Fast, s.r.o.	není	nájemníci	osobní údaje	listinné i digitální	SSB2000
Pronájem nemovitostí	**28**	Účelem zpracování je vedení záznamů o pronajímatelích	nikdo	nikdo	občané	osobní údaje	listinné i digitální	Word, Excel
Evidence čísel popisných	**29**	Účelem zpracování je vedení evidence žadatelů popisných čísel	nikdo	Městský úřad Chodov	žadatelé	osobní údaje	listinné i digitální	Word, Athena
Evidence vlastníků společenství jednotek	**30**	Účelem je zpracování osobních údajů v souvislosti se správou vlastníků společenství jednotek	Koncept Fast s.r.o., Starlit s.r.o, Credit One, a.s., Mgr. MUDr. Pavel Strejc	výbor společenství vlastníků jednotek	občané města	osobní údaje	listinné i digitální	SSB2000
Stížnosti	**31**	Účelem zpracování je evidence stížností občanů	PilsCom s.r.o., Changroup s.r.o.	obyvatelé města případně jiný klient	obyvatelé města případně jiný klient	osobní údaje	listinné i digitální	Athena, Word
Vedení účetnictví	**32**	Zpracování osobních údajů v souvislosti s evidencí a oběhem účetních dokladů	Triada s.r.o.	nikdo	zaměstnanci, dodavatelé, příjemci dotací, osoby kterým vznikl závazek vůči obci	osobní údaje	listinné i digitální	Munis
Vidimace a legalizace	**33**	Zracování osobních údajů v souvislosti s výkonem státní správy v oblasti ověřování příslušných dokumentů	Triada s.r.o.	nikdo	fyzické osoby, žadatelé	osobní údaje	listinné i digitální	Munis

Volební seznamy a průkazy	***34***	*Účelem zpracování osobních údajů je evidence voličů a voličských průkazů.*	*ChanGroup s.r.o. , TRIADA, s.r.o.*	*okrskové volební komise*	*občané*	*osobní údaje*	*listinna*	*není*
Vymáhání pokut a pohledávek	***35***	*Vedení evidence pohledávek, nedoplatků a penále*	*není*	*banky, spořitelny ČSSZ, zdravotní pojišťovny*	*obyvatelé*	*osobní údaje*	*listinná*	*není*
Vyzvedávání receptů	***36***	*Identifikace osob, kterým se poskytuje služba vyzvedávání receptů*	*není*	*není*	*obyvatelé=senioři*	*osobní údaje*	*listinná i digitální*	*Word*
Dokumentace jednání Rady a Zastupitelstva města	***37***	*Účelem zpracování je vedení dokumentace pro jednání RM, ZM a jejich komisí.*	*není*	*není*	*zaměstnanci, obyvatelé obce a jiní obyvatelé ČR*	*osobní údaje*	*listinná i digitální*	*Word*
Ztráty a nálezy	***38***	*Evidence osobních údajů v souvislosti s řešením ztracených-nalezených předmětůna katastru města*	*Triada s.r.o.*	*není*	*občané města (předpokládá se)*	*osobní údaje*	*listinná i digitální*	*SW Athena, Word*
Zvláštní příjemce důchodu	***39***	*Správní řízení - ustanovení zvláštního příjemce důchodu*	*není*	*Česká správa sociálního zebezpečení*	*příjemce důchodu, zvláštní příjemce důchodu*	*osobní údaje + údaje zvláštní kategorie*	*listinná*	*Word*

5. Vyhodnocení souladu s principy GDPR

Sumární komentář.

Pro každou agendu byl vypracován hodnotící formulář, který přehledně dokladuje vyhodnocení informací se sběrných formulářů, popisujících stávající stav a to z hledisek jestli:

1. Je vytvořen popis zpracování osobních údajů agendy ?
2. Je vytvořen popis zpracovávaných osobních údajů ?
3. Jsou zavedena technická opatření ochrany osobních údajů ?
4. Jsou zavedena organizační opatření ochrany osobních údajů ?
5. Jsou dodržovány základní principy ZOÚ ?
6. Je vedená odpovídající dokumentace ?

Stav agend z hlediska prvních dvou tematických oblastí vyhodnocování vykazuje u velké většiny agend dobrou připravenost a soulad s požadavky Obecného nařízení (GDPR). V některých případech pouze není jasně a srozumitelně popsán účel zpracování osobních údajů a stejně popis zpracování osobních údajů (kdo je zdrojem údajů, jak se údaje zpracovávají a v jakém prostředí). Doporučujeme tyto popisy sjednotit.

V oblasti technických opatření je nejčastějším nedostatkem nedostatečné zabezpečení dokumentů v listinné podobě. Dokumenty jsou často volně uložené v nezamčené skříni, přesto, že v některých případech se to týká i údajů zvláštní kategorie. Není rovněž nastaven klíčový režim, který by řešil evidenci a oprávněnost užívání klíčů. Opakovaným nedostatkem je skutečnost, že řízený přístup do PC, LAN a některých aplikací je sice řešen prostřednictvím uživatelského jména a hesla, ale uživatelská hesla mají trvalou platnost. Není nastavena politika ochrany a režimu pravidelné obměny hesel.

V oblasti organizačních opatření je hlavním nedostatkem absence jmenování Pověřence pro ochranu osobních údajů (DPO). Dle čl. 36 odst.1 písm. a) nařízení EU 2016/679 má Správce (Město Toužim) povinnost tuto funkci ke dni 26.5.2018 zřídit. Dalším opakovaným nedostatkem z oblasti organizačních opatření jsou nezavedené procesy pro naplňování práv subjektů údajů, řešení bezpečnostních incidentů ochrany osobních údajů a pravidelného proškolování a s tím spojené vedení příslušné povinné dokumentace. Během analýzy se projevila skutečnost, že zaměstnanci Správce - oprávněné osoby pro zpracování osobních údajů, mají nedostatečné povědomí o principech a nařízeních souvisejících s ochranou osobních údajů a s jejich zpracováním.

Nejčastějším nedostatkem stávajícího stavu zpracování osobních údajů z hlediska dodržování základních principů zpracování (minimalizace, důvěrnost, dostupnost, integrita, odolnost, transparentnost, zákonnost) je používání pomocných souborů ve formátu word a excel, které obsahují osobní údaje. Tyto soubory nejsou nijak chráněné a jsou ukládané na různé paměťové média blíže nespecifikovanou dobu. Není tím zajištěn princip minimalizace zpracování jak z hlediska doby, tak z hlediska účelu zpracování (zpracování po nezbytně dlouhou dobu a pouze daný účel) a je ohroženo hledisko integrity, odolnosti a důvěrnosti zpracovávaných osobních údajů.

Největší nedostatky vykazuje stávající stav zpracování osobních údajů u všech agend z hlediska stavu existence a vedení dokumentace o zpracování osobních údajů. Nejsou vedené záznamy o činnostech zpracování osobních údajů, není zavedená odpovídající dokumentace procesů pro naplňování práv subjektů údajů, řešení bezpečnostních incidentů ochrany osobních údajů a pravidelného proškolování. Není popsaná politika ochrany přístupových hesel (četnost obnovy, důvěrnost, složitost..) a popsán a nastaven řízený přístup do vyhrazených prostor, včetně zásad pro klíčový režim (evidence, oprávněnost...) Smluvní dokumenty (souhlasy, smlouvy, vzorové žádosti…) Správce se Subjektem údajů, případně se Zpracovatelem ve stávajícím stavu neodpovídají principům Obecného nařízení a je potřeba je přepracovat do souladu. Do vzorových smluv, žádostí a formulářů dát v souladu s principem transparentnosti informaci o účelu a době zpracování, včetně práv SÚ. Zavést pravidla pro vytváření interních dokumentů (formulářů/žádostí/smluv), které by obsahovali osobní data, včetně nutnosti konzultace s DPO. Vodítkem pro úpravu těchto dokumentů můžou být doporučení uvedená v přílohách tohoto dokumentu. (*Příloha č.4 - Principy souhlasu, Příloha č.5 - Principy smlouvy se Zpracovatelem*)

Řešení těchto nedostatků a nesouladu s požadavky Obecného nařízení (GDPR), bude muset Správce věnovat zvýšené úsilí, v závislosti na jeho technických a organizačních možnostech a s přihlédnutím na priority řešení jednotlivých nedostatků tak, aby se pokud možno co nejdříve dostal do souladu s požadavky Obecného nařízení (GDPR) alespoň v základních hodnotících bodech.
Konkrétnější popis jednotlivých nedostatků a doporučená opatření obsahují jednotlivé hodnotící tabulky, které jsou součástí tohoto dokumentu v příloze. (*Příloha č.2 – Vyhodnocení souladu stávajícího stavu s GDPR u jednotlivých agend*)

Analýza potvrdila, že Správce podcenil organizační a technická opatření, jak v oblasti obecného povědomí o bezpečnostní politice, s důrazem na bezpečnostní politiku ochrany osobních údajů, jako významného aktiva Správce, tak z hlediska popisu činností zpracování, nastavení potřebných procesů a vedení dokumentace k těmto procesům. Správce nemá dostatečné povědomí o hrozbách a výši možných rizik zneužití u zpracovávaných osobních údajů.

Kromě výše uvedených všeobecných nedostatků a doporučení jejich odstranění, auditor předkládá dále následná všeobecná doporučení:

DA1: Auditor doporučuje, aby u agend, které pracují s citlivými osobními údaji, byla zvážená nutnost provedení analýzy rizik.

DA2: Auditor doporučuje, v rámci transparentního přístupu Správce k Subjektům údajů, o kterých zpracovává osobní údaje, proaktivně zpracovat ucelený přehledný materiál informující o rozsahu, účelu, formě zpracování osobních údajů v jednotlivých agendách, včetně uvedení mandátu (právního základu) zpracování, který by byl určený jako základní informace Subjektům údajů a volně přístupný např. prostřednictvím www stránek Správce. (případně byl součástí příslušné interní směrnice)

DA3: Auditor doporučuje, aby nejpozději do 6 měsíců provedl Správce opakovanou, postanalýzu stavu zpracování osobních údajů u svých identifikovaných agend s cílem zjištění stavu odstranění identifikovaných nedostatků a naplnění potřebných opatření.

DA4: Auditor doporučuje, v rámci postanalýzy na základě provozních zkušeností přehodnotit počet a nutnost evidence některých agend, které mají stejný, nebo podobný účel a způsob zpracování (matriky – agendy 10, 11, 12 a 17, vyřizování žádostí, nájmy…atd) s cílem sloučení některých podobných agend, případně zrušení některých agend zavedením jiných organizačních opatření, což by mohl přispět ke snížení administrativy při vedení povinné dokumentace zpracování osobních údajů.

6. Návrh priorit realizace jednotlivých opatření

Jednotlivá opatření budou odvislá od konkrétních technických, organizačních, personálních kapacit správce. Auditor navrhuje nápravná řešení realizovat dle priorit, v závislosti na míře nesouladu v kritických bodech, s ohledem na směrnici EU následovně:

- jmenování Pověřence pro ochranu osobních údajů, včetně jeho vhodné prezentace vůči Subjektům údajů a nastavení interních pravidel zajišťujících Pověřenci potřebné podmínky a součinnost ze strany všech zaměstnanců, zejména při poskytování informací a dokumentů nutných k plnění jeho úkolů.

- odstranění nesouladu při dodržování základních principů zpracování z hlediska minimalizace, důvěrnost, dostupnosti, integrity, odolnosti, transparentnosti a zákonnosti. Zejména, pokud byl identifikován nedostatek z hlediska správného právního základu zpracování osobních údajů (např. špatný stávající právní základ, neexistující/nevyhovující souhlas…)

- zavedení šifrování osobních údajů u dotčených agend

- definování postupů pro řešení bezpečnostních událostí a incidentů, včetně zavedení dokumentace nastavení vhodných komunikačních kanálů (e-mail, www formulář, helpdesk) a určení odpovědných osob.

- definování procesů pro naplňování práv SÚ, včetně zavedení dokumentace a nastavení vhodných komunikačních kanálů (e-mail, www formulář, helpdesk) a určení odpovědných osob.

- doplnění zaměstnanecké smlouvy ujednáním o mlčenlivosti se zpracováním osobních údajů, případně o správné znění souhlasů se zpracováním osobních údajů

- doplnění smluv se zpracovateli o ujednání ohledně zpracování osobních údajů

- nastavení dalších procesů, které vykazují nedostatky, nebo nesoulad (proškolování, klíčový režim, politika nastavování a aktualizace hesel… atd. podrobněji viz nedostatky uvedené ve vyhodnocovacím formuláři u každé agendy v příloze č.2)

- zpracování interní dokumentace v bodech, kde vykazuje absenci, nedostatky, nebo nesoulad (aktualizace směrnice pro ochranu osobních údajů, vedení záznamů o činnostech zpracování osobních údajů (ZOÚ), evidence proškolování, evidence klíčů režim, evidence bezpečnostních incidentů, dokumentace popisující podpůrné aktiva pro ZOÚ a jejich ochranu… atd. podrobněji viz nedostatky uvedené ve vyhodnocovacím formuláři u každé agendy v příloze č.2)

- zavedení vhodných technických a organizačních opatření pro odstranění identifikovaných nedostatků v této oblasti (např. fyzické zabezpečení dokumentů v listinné podobě v zamykatelných skříních, včetně definování klíčového režimu, zabezpečení dat při přenosu, podrobněji viz nedostatky uvedené ve vyhodnocovacím formuláři u každé agendy v příloze č.2)

- zavést formou interních pravidel zásadu pravidelného prověřování dodržování nastavených mechanizmů pro zpracování osobních údajů, včetně provádění pravidelné analýzy stavu souladu s GDPR.

Zpracování interní dokumentace doporučujeme řešit s odborně způsobilým subjektem (např. právníkem, IT manažerem, bezpečnostním technikem, pověřenec pro ochranu osobních údajů…). U subjektů, které mají ze zákona povinnost jmenovat Pověřence pro ochranu osobních údajů (DPO), je konzultace s DPO pro tvorbu interní dokumentace dle obecného nařízení povinná.

Přílohy

1. **Sběrné formuláře k jednotlivým agendám**
2. **Vyhodnocení souladu s GDPR u jednotlivých agend**
3. **Seznam relevantních zákonů**
4. **Principy souhlasu**
5. **Principy smlouvy se Zpracovatelem**
6. **Základní školící materiál GDPR**
7. **Prezenční listina školení**