Druh dokumentu/ Type of the document	*Označení dokumentu/ Document Number*
Zpráva/ Report	**Z201710004-GDPR-MUVidnava**

Název/ Title:

Úvodní audit připravenosti pro soulad s nařízením GDPR

v organizaci

Město Vidnava

vstupní analýza

Zpracovatel/ Processor:	*Schválil/Approved by:*
Mgr. Ivana Tilkeridu	**Bc. Radek Kubíček, MBA**
auditor	*vedoucí auditor*

INTERNÍ DOKUMENT

URČENO POUZE PRO MĚSTSKÝ ÚŘAD VIDNAVA. TATO ZPRÁVA NEBUDE POSKYTOVÁNA ŽÁDNÝM TŘETÍM OSOBÁM.

Datum vydání/ Date of issue: **10.10.2017**

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

OBSAH DOKUMENTU

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

1. IDENTIFIKACE ORGANIZACE/ *Identification of the organization*

Název organizace (dle OR)/ Organization Město Vidnava

IČ/ Registration Number: 003035854

Adresa/Address: Mírové nám. 80, 790 55 Vidnava

Rozsah auditu/ Scope of audit:

Úvodní audit připravenosti pro soulad s nařízením GDPR

Vrcholové vedení / Top management: Bc. Rostislav Kačora, starosta

Místo organizace, kde byl prováděn audit/ The premise, where the audit has been done:

Mírové nám. 80, 790 55 Vidnava

Organizace obce zahrnuté do auditu/ Organisations included into the audit:	*Adresy poboček organizace/ Other production premises:*	*Počet zaměstnanců/ Number of employees:*
Městský úřad Vidnava	Mírové nám. 80, 790 55 Vidnava	25–49

2. IDENTIFIKACE AUDITU/ *Audit Identification*

Typ auditu/abrev.	*Úvodní analýza Initial Audit*	*Následný audit Follow-up Audit*	*Systémový audit System Audit*	*Situační audit Situation Audit*
GDPR	☒	☐	☐	☐

Začátek auditu/ Beginning of the audit: 13.09.2017

Konec auditu/ End of the audit: 10.10.2017

Tým auditorů/ Audit Team:

Bc. Radek Kubíček, MBA *Vedoucí auditor/ Lead auditor*

Mgr. Ivana Tilkeridu *Auditor/ 2nd auditor*

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

3. PŘEDMĚT AUDITU/ *Subject of the audit*

„Úvodní audit připravenosti pro soulad s nařízením GDPR“ si klade za cíl zjištění současného stavu připravenosti agend, provozní dokumentace a zabezpečení osobních údajů v rámci stávajícího systému vůči plánovanému nařízení GDPR (vstupujícího v platnost v květnu 2018) ve Městě Vidnava. Do auditu byl zahrnut **Městský úřad Vidnava** (viz bod 1 – Identifikace organizace)

Výstupem předmětu plnění je zhodnocení stávajícího systému ochrany osobních údajů v následujících oblastech a návrh opatření:

1. Zjištění zpracovávaných agend na městském úřadu
2. Zjištění typů zpracovávaných osobních údajů s ohledem na platnou legislativu
3. Zjištění nastavení používaných IT zařízení z bezpečnostního hlediska
4. Návrh opatření, která je nutno podniknout k zajištění souladu s nařízením GDPR

4. POUŽITÉ METODY A POSTUPY při zpracování auditu/ *Used Process Audit Techniques and Methods*

„Úvodní audit připravenosti pro soulad s nařízením GDPR“ ve městě Vidnava byl realizován v prostředí Městského úřadu Vidnava v termínu od 13. 09. 2017 do 10. 10. 2017. Audit probíhal podle předem připraveného a odsouhlaseného harmonogramu.

4.1 Kontrola provozní dokumentace

V průběhu auditu jsme se zaměřili na posouzení stavu provozní dokumentace, pracovních smluv a smluv uzavřených s dodavateli a poskytovateli služeb. Dále jsme se věnovali způsobům zacházení s osobními údaji a s evidencí souhlasů se zpracováním osobních údajů.

4.2 Kontrola IT zařízení

Součástí úvodního auditu bylo posouzení kybernetické bezpečnosti používaných zařízení a zjištění hrozeb úniku osobních dat. Předmětem kontroly bylo také zjišťování způsobu šifrování a zálohování dat a vytváření kopií na přenosné datanosiče.

4.3 Individuální polostrukturovaný rozhovor

Individuální polostrukturovaný rozhovor slouží ke zjištění reálného stavu stávajícího systému nakládání s osobními údaji. Metoda umožňuje vyhledat slabá místa systému a určit míru hrozby úniku osobních dat ze strany zaměstnanců městského úřadu.

4.4 Dotazníkové šetření

Dotazníkové šetření jsme realizovali mezi zaměstnanci Městského úřadu Vidnava, včetně starosty (statutárního zástupce), vedoucích jednotlivých odborů a interního správce počítačové sítě.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

5. TYPY ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ

Město Vidnava zpracovává osobní údaje v rozsahu stanoveném zákony v platném znění, zejména podle zák. č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, zák. č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání, zák. č. 128/2000 Sb., o obcích, zák. č. 563/1991 Sb., o účetnictví, zák. č. 565/1990 Sb., o místních poplatcích atd. Osobní údaje, které nejsou zpracovávány ve veřejném zájmu, se zpracovávají na základě smluv nebo souhlasů se zpracováním osobních údajů.

Na Městském úřadě Vidnava jsou zpracovávány obecné, organizační i citlivé osobní údaje. Mezi základní osobní údaje, které město Vidnava zpracovává patří jméno, příjmení, datum narození, rodné číslo, bydliště, zdrav. pojišťovna, číslo účtu, IČ, DIČ, sídlo (u firem), telefon, e-mail, datová schránka aj.

V rámci organizace je určena klasifikace dat např. na utajované informace, povinně zveřejňované informace, osobní či citlivá data pod. Klasifikace dat je stanovena na základě zákonné povinnosti.

Organizace získává referenční údaje, tj. právně závazné údaje ze základních registrů ROS (= Registr osob), ROB (=Registr obyvatel), RÚIAN (= Registr územní identifikace, adres a nemovitostí) nebo RPP (= Registr práv a povinností) prostřednictvím svých agendových informačních systémů. Informace a osobní data, která jsou v organizaci zpracovávána, jsou tedy získávána od institucí veřejné zprávy, ale také přímo od občanů.

6. FORMY UCHOVÁVÁNÍ OSOBNÍCH ÚDAJŮ NA MĚSTSKÉM ÚŘADĚ VIDNAVA

6.1 Listinná evidence

Údaje uchovávané v listinné podobě	Místo uložení
osobní údaje zaměstnanců (pracovní smlouvy, platové výměry, diplomy, certifikáty,…)	Personální oddělení
provozní dokumentace (smlouvy, technická dokumentace,…)	Kancelář starosty, oddělení matriky, pracovna technika
evidence obyvatel	Matrika, podatelna
nájemní smlouvy z bytové agendy	SOBYT (Správa obecních bytů)
údaje o klientech (žádosti o umístění v DPS, rozhodnutí,…)	Podatelna
Technická dokumentace požární techniky	Pracovna technika

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

Ruční záznamy k jednotlivým agendám jsou v listinné podobě uchovávány v příručním nebo centrálním archivu, který je umístěn v budově městského úřadu. Spisovna se nachází v přízemí budovy úřadu a je zabezpečen pouze zámkem. Jiné zabezpečení proti vniknutí či v případě neočekávaných událostí není zajištěno. Přístup do spisovny mají všichni zaměstnanci úřadu.

6.2 Elektronická evidence

Pro přístup k záznamům z jednotlivých agend jsou využívány rovněž agendové informační systémy (KEO). Databáze k používanému softwaru jsou uloženy a zálohovány na serveru organizace. Podrobněji o nastavení používaných IT zařízení, formách elektronických záloh a nastavení serveru viz bod 7.

6.3 Archivace a uložení listinných dokumentů

Uložení dokumentů v organizaci je realizováno na několika úrovních. Dokumenty, které nejsou určeny k archivaci nebo jsou využívány pravidelně (platné smlouvy, evidence osob apod.) jsou umístěny přímo v kancelářích jednotlivých zaměstnanců. Většinou se jedná o příruční skříně, stolky a zásuvky, z nichž některé nejsou uzamykatelné.

Spisovna pro uložení listinných dokumentů je umístěna v přízemí budovy úřadu. Jeho zabezpečení je zajištěno pouze standardním zámkem, k němuž mají klíče všichni zaměstnanci úřadu.

Pouze část vedené evidence je uchovávána formou digitalizace a zálohována. Systém obnovy listinných dokumentů v případě neočekávaných událostí nebo při zásahu vyšší moci tedy není dostačující, neboť umožňuje obnovu údajů z archivu jen z malé části.

7. ZJIŠTĚNÍ NASTAVENÍ POUŽÍVANÝCH IT ZAŘÍZENÍ

7.1 Server a jeho zabezpečení

Hlavním prvkem IT infrastruktury města je fyzický server. Server je umístěn v uzamčeném racku na chodbě Městského úřadu Vidnava. Klíče od serverovny jsou k dispozici u starosty a interního IT správce.

Data serveru jsou uložena na dvou zrcadlených discích, které jsou spojené do pole RAID 1. Proti výpadku elektrického proudu je server chráněn záložním zdrojem. Na serveru je nainstalován serverový operační systém Windows 7 Professional. Server obsluhuje tyto role:

- Server pro sdílené síťové složky
- Aplikační server

Zálohování serveru probíhá 1x týdně na oddělený HDD. Na serveru jsou provozovány všechny informační systémy (aplikace). V organizaci je používáno cloudové řešení a autentizace pomocí autentizačních tokenů.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

7.2 Nastavení jednotlivých stanic a používaný software

Na Městském úřadě Vidnava je v tuto chvíli používáno 6 pevných stolních počítačů. Pracovní stanice jsou sice opatřeny přístupovým heslem, nicméně ta nejsou unikátní. Na třech pracovních stanicích je nainstalován operační systém Windows 10, na zbylých třech Windows 7. Na všech pracovních stanicích je nainstalován antivirový program ESET Secure Office. V případě problému/virové nákazy je pak ze stanice odeslán informativní e-mail správci sítě.

Na pracovních stanicích jsou nainstalovány databázové informační systémy jako např. KEO, které jsou provozovány na serveru města. Aplikace slouží k přístupu do jednotlivých agend. Přístup do agend je zabezpečen heslem, přičemž každý ze zaměstnanců má přístup pouze k agendám, které potřebuje pro výkon činnosti.

Vzhledem k výše zmíněným účelům serveru je zřejmé, že se na něm nacházejí citlivé osobní údaje. Tyto údaje se mohou nacházet jednak v dokumentech, které na server ukládají pracovníci městského úřadu, tak v informačních systémech, které jsou na serveru provozovány. K uložení dat těchto informačních systémů se využívá databází. Jelikož se v organizaci pracuje s osobními údaji, tak je potřeba zajistit aby dokumenty, které obsahují osobní údaje, byly uloženy na předem definovaných místech a přístup k těmto složkám a dokumentům měli pouze oprávnění uživatelé.

7.3 Zabezpečení sítě a vzdálené přístupy

Veškeré počítačové stanice v této organizaci jsou propojeny do sítě. K počítači se může přihlásit kdokoliv, neboť žádný z počítačů není zabezpečen heslem. Navíc není na lokálních pracovních stanicích používána doménová politika s řízeným oprávněním, na počítače tak může kdokoliv cokoliv svévolně naistalovat.

Vzdálené přístupy na počítačové stanice nejsou umožněny ani zaměstnancům, ani IT pracovníkovi.

7.4 Připojení k internetu

Připojení k internetu je zajištěno od společnosti Web4soft s.r.o. přes optické nebo ethernetové přípojky. V rámci organizace je zřízena i wi-fi síť, která je zabezpečena heslem.

7.5 Elektronická pošta

Na většině lokálních počítačových stanic je pracovníky úřadu používán poštovní klient Microsoft Outlook, na jedné ze stanic Windows Live Mail. Pro každého uživatele je vytvořena firemní schránka *@vidnava.cz*, která je zabezpečená heslem. Po stažení do poštovních klientů na počítačích pracovníků jsou e-maily ze serveru smazány. Šifrování zpráv se v rámci e-mailové komunikace nepoužívá.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

7.6 Kamerový systém

Ve městě je instalováno devět bezpečnostních kamer. Dvě kamery jsou umístěny na náměstí Míru, jedna kamera na budově bytového družstva, jedna na budově školy, jedna u sběrny surovin, jedna na veřejných toaletách, jedna u čistírny odpadních vod, jedna na budově kostela a jedna kamera na budově informačního centra. Na všech místech je viditelně umístěno upozornění na používání kamerového systému. Záznamy z kamer se archivují 14 dní.

8. PRÁCE S OSOBNÍMI ÚDAJI A DOSTUPNOST DAT

Nařízení Evropského parlamentu o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR) mj. posiluje práva subjektů údajů (občanů) na informace o tom, jakým způsobem jsou jeho osobní údaje evidovány a zpracovávány. Ve chvíli kdy subjekt dat bude požadovat tyto informace, je potřeba mít možnost projít veškerá možná úložiště těchto údajů a tyto osobní údaje vyhledat.

Bohužel na úřadě chybí možnost systematického prohledávání všech agend a dokumentů tak, aby byl umožněn snadný přístup k osobním údajům subjektů dat.

S právem na informace, úpravu nebo výmaz osobních údajů souvisí potřeba zajistit dostupnost osobních údajů. Data by měla být především chráněna proti výpadku elektrického proudu, což je na úřadě zajištěno záložním zdrojem, a také proti výpadku/chybě HW. Samozřejmostí by mělo být pravidelné a dostatečné zálohování těchto dat (o zálohování dat viz výše v kapitole 8).

Pro splnění práv subjektů dat bude nutné vytvořit systematizovaný přehled úložišť, dokumentů a databází, ve kterých se osobní údaje nacházejí, aby bylo možné v případě žádostí o informace v co nejkratším možném termínu přehled zpracovávaných údajů předložit, a to včetně uvedení právního titulu, na jehož základě jsou data zpracovávána (podrobněji viz níže v kapitole Závěrečné zhodnocení a návrh opatření).

9. REVIZE DOKUMENTŮ

V rámci vstupní analýzy byla provedena revize pracovně-právních dokumentů, smluv, žádostí, přihlášek a souhlasů se zpracováním osobních údajů a také revize směrnic a vnitřních předpisů upravujících chod organizace (jmenovitě viz Příloha č. 1).

Některé dokumenty obsahují nepřesné formulace udělení souhlasu se zpracováním osobním údajů, jež nemají oporu v zákoně nebo obsahují údaje, které nejsou nezbytně nutné pro zpracování dané agendy bez jakéhokoliv vysvětlení účelu zpracování nebo specifikace doby, po kterou budou data uchovávána. Některé dokumenty – především pracovní smlouvy, pak obsahují redundantní souhlas se zpracováním osobních údajů nutných pro mzdové účetnictví a vyplývající ze zákoníku práce, nebo jež vymezují jiné právní normy.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

9.1 Revize pracovně-právních dokumentů

Smlouvy zaměstnanců na hlavní pracovní poměr obsahují nadbytečný souhlas pro zpracování osobních údajů, protože definovaný účel v tomto souhlasu je totožný se zákonnou povinností. Pracovní náplň a platový výměr obsahují pouze organizační osobní údaje související s výkonem činnosti zaměstnance.

9.2 Revize smluv

Během auditu byla provedena revize smluv, které jsou uzavírány s fyzickými osobami a obsahují tedy osobní údaje. Seznam revidovaných smluv je uveden v Příloze č. 1 této zprávy. Revidované smlouvy obsahují pouze takové osobní údaje, které jsou nezbytné pro naplnění předmětu smlouvy.

9.3 Revize žádostí, přihlášek a souhlasů se zpracováním osobních údajů

Většina dokumentů tohoto typu obsahuje právní titul, na jehož základě jsou osobní údaje shromažďovány a zpracovávány. Je však nutné zrevidovat, zda všechny požadované údaje jsou pro zpracování dané agendy nezbytně nutné a v případě, že nemají oporu v zákoně, vyčlenit je v rámci formuláře s možností udělení/ neudělení souhlasu se zpracováním osobních údajů včetně účelu zpracování a doby, po kterou budou data uchovávána.

Název dokumentu	Příklady údajů, které nejsou nezbytně nutné pro zpracování agendy a měly by být ošetřeny souhlasem
Žádost o osvobození místního poplatku za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů	Telefonní kontakt, e-mail

9.4 Revize směrnic, vnitřních předpisů a řádů

K revizi v rámci vstupního auditu byly předloženy čtyři aktuálně platné směrnice a vnitřní řády (seznam dokumentů viz Příloha č. 1). Žádná ze směrnic ani vnitřních řádů neupravuje práci s osobními údaji. Koncepčně zpracovaná směrnice týkající se zpracování, ochrany a nakládání s osobními údaji v organizaci chybí.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

10. VÝSLEDEK DOTAZNÍKOVÉHO ŠETŘENÍ MEZI ZAMĚSTNANCI

Dotazníkové šetření probíhalo mezi 3 zaměstnanci městského úřadu, kteří pracují s osobními údaji. Cílem dotazníku bylo zjistit chování jednotlivých zaměstnanců úřadu ve vztahu k bezpečnosti při práci s osobními údaji.

Jednotlivé kanceláře se při odchodu vždy zamykají. Nicméně téměř všichni zaměstnanci úřadu odkládají listinné dokumenty do příručních skříní, stolků či zásuvek, z nichž některé nejsou uzamykatelné, takže by k úniku dat mohlo dojít. Nepotřebné listinné dokumenty obsahující osobní údaje jsou po použití důsledně skartovány, z čehož lze soudit, že si zaměstnanci úřadu plně uvědomují nutnost obezřetnosti při nakládání s osobními údaji během výkonu své práce.

Třetí blok otázek byl věnován chování zaměstnanců při využívání počítačů a jednotlivých agendových informačních systémů. Počítače v organizaci jsou sice opatřeny přístupovými hesly, nicméně ta nejsou unikátní (rozlišování malých/velkých písmen, prokládání číslicemi nebo jinými znaky, alespoň 8 znaků) a jsou známa i dalším pracovníkům úřadu (IT pracovníkovi nebo kolegovi/kolegyni), navíc si tito lidé svá hesla pravidelně nemění.

Zaměstnanci mají pouze přístup do svých agend. V rámci organizace není umožněn vzdálený přístup, což snižuje riziko úniku dat. Někteří zaměstnanci však nemají přesný přehled o tom, která data jsou v jednotlivých agendách podložena zákonem a která jsou „navíc“. Někteří zaměstnanci si také vytváří elektronické kopie dokumentů obsahujících osobní údaje pro práci mimo pracoviště.

Zaměstnanci prozatím nepodstoupili školení k problematice GDPR ani se o problematiku sami aktivně nezajímají.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

11. ZJIŠTĚNÉ NEDOSTATKY

Na Městském úřadě Vidnava byly zjištěny následující nedostatky:

- Nedostatečná znalost nařízení GDPR ze strany zaměstnanců Města Vidnava (zaměstnanci dosud nebyli řádně proškoleni);
- Město Vidnava nesplňuje registrační povinnost vyplývající ze zákona č. 101/2000 Sb. o ochraně osobních údajů
- Budova Městského úřadu není proti vniknutí zabezpečena alarmem;
- Nedostatečná kontrola, kdo a jak s daty zachází, neexistující monitoring přístupových práv do agend osobních údajů. Městský úřad neprovádí kontrolu, zdali má osoba přístup tam, kam by měla mít;
- Nejsou posouzena rizika spojená se zpracováním osobních údajů a nejsou přijata opatření ke zmírnění těchto rizik;
- Všeobecné souhlasy se zpracováváním osobních údajů nejsou zpracovány systémově a v souladu s nařízením GDPR;
- Nejsou nastaveny procesy pro bezodkladné oznámení narušení bezpečnosti osobních údajů;
- Neexistuje postup pro výmaz údajů plynoucí z práva být zapomenut;
- Nejsou stanoveny lhůty pro uchování osobních údajů pro nezbytně nutnou dobu a lhůty pro výmaz;
- Není zajištěn bezpečný proces exportu a importu osobních údajů mezi poskytovateli služeb;
- Neexistují pravidla pro nakládání s informacemi – např. neukládat informace na vlastní USB a tím vytváření kopií v nezašifrované formě;
- Nedostatečná provázanost informačních systémů pro rychlé a jednoduché poskytnutí komplexních informací a zajištění přístupu k vlastním osobním údajům subjektů dat;
- Neexistují plány obnovy dat při haváriích a v nepředvídatelných situacích při zásahu vyšší moci - část dokumentů existuje jen v papírové podobě, nejsou jiným způsobem zálohovány, tudíž při ztrátě nebo zničení údaje nelze obnovit;
- Nedostateční zabezpečení listinných dokumentů v příručních archivech – v kancelářích jsou uloženy papírové kopie obsahující osobní údaje;
- Není nastaven proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

12. ZÁVĚREČNÉ ZHODNOCENÍ A NÁVRH OPATŘENÍ

Na základě námi provedeného auditu musíme konstatovat, že existuje v souvislosti s novým nařízením GDPR řada nedostatků při zpracovávání osobních údajů ve městě Vidnava. Nedostatky v zajištění ochrany osobních údajů jsou způsobeny především minimální znalostí nové legislativy, nedostatečným proškolením zaměstnanců a absencí systematizovaných zabezpečených procesů správy dat.

V oblasti vlastního zabezpečení a zajištění adekvátní ochrany osobních údajů v elektronické evidenci je zapotřebí přesně zmapovat logickou strukturu zapojení IT, strukturu ukládání a zálohování dat, správné nastavení oprávněného přístupu k osobním údajům tak, aby bylo zamezeno svévolnému nakládání s nimi nepovolanými osobami.

Zvýšená pozornost musí být věnována také zajištění fyzické ochrany prostor, v nichž se s osobními údaji nakládá, a to ochrany kanceláří, archivu apod. Především v prostorách městského úřadu je zvýšený pohyb cizích osob, které se v budově mohou pohybovat bez dozoru.

I přes výše uvedené nedostatky je patrné, že jsou pracovníci městského úřadu Vidnava znalí problematiky zpracovávaných agend, jsou si vědomi, jaké osobní informace zpracovávají a ve velké míře se snaží omezit získávání osobních údajů na nezbytně nutné údaje, které jim ukládá zákon. Zaměstnanci a představitelé města, kteří pracují s citlivými daty, jsou si vědomi zvýšené opatrnosti při nakládání s nimi i důsledků jejich případné ztráty nebo úniku.

Veškeré zjištěné nedostatky musí splňovat nejen nařízení GDPR, ale také Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.

12.1 Návrh opatření pro zajištění shody s nařízením GDPR

12.1a Procesní opatření

1. Analýza rizik spojených se zpracováním osobních údajů.
2. Vytvoření seznamu jednotlivých zákonných požadavků, kterými se jednotlivé agendy řídí, tudíž k jejich získání nebude město potřebovat souhlas subjektu se zpracováním osobních údajů.
3. Systematizace souhlasů se zpracováním osobních údajů a jejich přepracování v souladu s nařízením GDPR. Souhlasy se zpracováním osobních údajů nesmí být součástí smluv ani obchodních podmínek.
4. Nastavení procesu pro řešení incidentů souvisejících s osobními údaji – informovanost úřadu na ochranu osobních údajů, provedení vlastní analýzy incidentu, podmínky pro informovanost subjektu údajů atd.
5. Zvážení uzavření pojištění odpovědnosti a pojištění kybernetických rizik, které nabízí právní ochranu proti kybernetickému útoku

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

6. Vytvoření dodatků smluv mezi správcem osobních údajů (Město Vidnava) a zpracovateli (dodavatelé software apod.) za účelem stanovení míry odpovědnosti v případě úniku osobních údajů

12.1b Organizační opatření

7. Důkladné proškolení zaměstnanců městského úřadu Vidnava v oblasti GDPR a ochrany osobních údajů, včetně bezpečnostních pravidel a postupů.
8. Vytvoření všech nezbytně nutných dokumentovaných postupů k řešení otázek souvisejících s právy subjektu údajů – žádosti, úpravy, výmaz, informovanost.
9. Zřízení pracovní pozice pověřence osobních údajů (DPO) nebo zajištění služeb DPO externím dodavatelem služeb.

12.1c Technická opatření

10. Nastavení procesu monitoringu přístupových práv do agend osobních údajů, pravidelná kontrola oprávněnosti přístupu jednotlivých zaměstnanců a zaznamenávání činnosti jednotlivých uživatelů (log management systémy s automatickým vyhodnocením logů – kdy, kdo a co dělal).
11. Systematizace bezpečnostních opatření a stanovení pravidel pro nakládání s informacemi a pro export a import osobních údajů, mezi poskytovateli služeb a jejich nastavení tak, aby nezatěžovaly pracovníky městského úřadu Vidnava.
12. Zlepšení fyzického zabezpečení kanceláří, serveroven a prostor, ve kterých se vyskytují osobní údaje subjektů údajů, aby byla adekvátním způsobem zajištěna jejich přiměřená ochrana, ochrana přístupu k datovým kabelům (mj. uzamykatelné kartotéky a skříně, bezpečné uložení klíčů, keypad nebo kamerový systém sledující serverovnu apod.)
13. Vytvoření plánu na zálohování dat a následných seznamů pro lepší lokalizaci jednotlivých údajů a vytvoření plánu na obnovení dat po haváriích a v nepředvídatelných situacích při zásahu vyšší moci.
14. Nástroje pro ochranu před škodlivým kódem (pokročilá antivirová řešení, heuristika, sandboxing atd.) a nástroje pro ochranu integrity komunikačních sítí (firewall/ IPS systém)
15. Nastavení procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
16. Návrh řešení provázanosti informačních systémů pro rychlé a jednoduché poskytnutí komplexních informací a zajištění přístupu k vlastním osobním údajům subjektů dat.
17. Zvážení možnosti zakoupení kryptografického softwaru pro šifrování e-mailů, dat na serverech, stanicích a mobilních zařízeních.
18. Zakoupení softwaru na evidenci osobních údajů dle GDPR.
19. Zabezpečení webových a mobilních aplikací před únikem osobních dat.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

13. HARMONOGRAM ČINNOSTÍ PRO IMPLEMENTACI GDPR OPATŘENÍ

do 01/ 2018	Vytvoření seznamu jednotlivých zákonných požadavků, kterými se jednotlivé agendy řídí
	Zpracování analýzy rizik
do 02/ 2018	Vytvoření směrnice týkající se ochrany osobních údajů a dalších nezbytně nutných dokumentovaných postupů, systematizace souhlasů se zpracováním osobních údajů
do 03/ 2018	Systematizace bezpečnostních opatření a stanovení pravidel pro nakládání s informacemi a pro export a import osobních údajů
04/ 2018	Seznámení zaměstnanců se směrnicí upravující ochranu osobních údajů v organizaci a školení se zaměřením na problematiku GDPR
do 05/2018	Nastavení procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření
do 05/2018	Zvážení možnosti zakoupení kryptografického software pro šifrování dokumentů a zakoupení software na evidenci osobních údajů dle GDPR.
od 05/ 2018	Jmenování/ přijetí (nového) zaměstnance na pracovní pozici pověřence osobních údajů (DPO) nebo zajištění služeb DPO externím dodavatelem služeb

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

14. PŘEDPOKLÁDANÉ NÁKLADY PRO IMPLEMENTACI GDPR OPATŘENÍ

Název opatření	Název varianty řešení	Částka
Zakoupení kryptografického software pro šifrování dokumentů		1 500,- Kč /zařízení
Zakoupení software na evidenci osobních údajů dle GDPR	Licence aplikace „Klement“ pro vedení agendy spojené s bezpečným provozováním IT infrastruktury. Je určená pro jeden subjekt. Není omezená doba využívání. Není omezen počet uživatelů. *VAE informační systémy s.r.o.*	135 000,- Kč
	Roční podpora a aktualizace aplikace „Klement“ (není nutná pro provozování zakoupené verze aplikace) *VAE informační systémy s.r.o.*	13 500,- Kč
Zajištění služeb DPO externím dodavatelem služeb – pouze MěÚ Vidnava *v termínu 05/2017-12/2017 (8 měsíců)*		80 000,- Kč
Zajištění služeb DPO externím dodavatelem služeb – včetně příspěvkových organizací *v termínu 05/2017-12/2017 (8 měsíců)*		160 000,- Kč
Zpracování analýzy rizik		15 000,- Kč
Zpracování směrnic na ochranu osobních údajů a metodiky pro získávání souhlasu se zpracováním osobních údajů		15 000,- Kč
Školení pro zaměstnance *v případě neposkytování služeb DPO společností 2K Consulting s.r.o.*		1 500,- Kč /osoba
Pojištění odpovědnosti a pojištění kybernetických rizik		10 000,- Kč

15. DOTAČNÍ MOŽNOSTI

V tuto chvíli bohužel neexistují dotační tituly, které by mohly alespoň částečně pokrýt náklady na kybernetickou bezpečnost a ostatní GDPR opatření, která bude ve Městě Vidnava nutné implementovat. Jednou z variant je výzva č. 10 IROP – Kybernetická bezpečnost, u níž je lhůta pro podání nabídek 22. 11. 2017. Minimální výše celkových způsobilých výdajů na projekt je však u této výzvy 2 000 000 Kč, což by bylo u Města Vidnava nerealizovatelné.

Společnost 2K Consulting s.r.o. se zavazuje informovat statutárního zástupce města o všech nových výzvách, které budou vyhlášeny po realizaci auditu, ale dříve než nabude účinnosti nařízení GDPR, pokud tyto výzvy budou odpovídat potřebám Města Vidnava.

2K CONSULTING
2K Consulting s.r.o.
Tovární 915/40
779 00 Olomouc - Hodolany
Tel: +420 775 110 979
E-mail: info@2kconsulting.cz
Web: www.2kconsulting.cz

Příloha č. 1. SEZNAM REVIDOVANÝCH DOKUMENTŮ

A. Pracovně právní dokumenty

- Pracovní smlouvy
- Pracovní náplň
- Platový výměr

B. Ostatní smlouvy

- Darovací smlouva
- Smlouva o poskytnutí dotace
- Smlouva o nájmu hrobového místa

C. Žádosti a přihlášky, souhlasy

- Ohlašovací povinnost k místnímu poplatku ze psů
- Žádost o vrácení přeplatku místního poplatku ze psů
- Ohlašovací povinnost o místním poplatku za provoz systému shromažďování, sběru, přepravy, třídění využívání a odstraňování komunálních odpadů.
- Žádost o vrácení přeplatku místního poplatku za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů na území města Vidnavy
- Žádost o osvobození místního poplatku za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů
- Souhlas se zpracováním osobních údajů – Vítání občánků
- Dotazník k uzavření manželství

D. Směrnice, vnitřní předpisy

- Směrnice o kontrole práce neschopných zaměstnanců
- Spisový a skartační řád pro Městský úřad Vidnava
- Směrnice upravující oběh účetních dokladů
- Místní řád Radnice BP-03-01