Město Horšovský Týn

Vnitřní předpis č. 4

Směrnice

o ochraně osobních údajů města Horšovský Týn

Zpracovala:	Ing. Eva Princlová, tajemnice MěÚ
Rozsah působnosti:	Město Horšovský Týn, Městský úřad Horšovský Týn
Účinnost:	7. 8. 2018
Počet stran:	40
Originál předpisu je uložen:	kancelář starosty
Elektronická podoba předpisu:	Intranetové stránky města
Vydal:	Ing. Eva Princlová, tajemnice MěÚ
Obdrží:	vedoucí odborů, kancelář starosty, knihovna, pečovatelská služba, MP

Obsah

1. Předmět úpravy směrnice

Tato směrnice stanoví základní pravidla a postupy pro zpracování a zabezpečení ochrany osobních údajů fyzických osob v rámci působnosti Města Horšovský Týn a Městského úřadu Horšovský Týn, dle **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** (dále jako „GDPR“ nebo „Nařízení“).

1.1 Použité zkratky

OÚ	osobní údaj/e
ZKOÚ	Zvláštní kategorie osobních údajů
SÚ	subjekt údajů (vlastník OU)
FO	fyzická osoba
ICT, IT	Informační a komunikační technologie
IS	Informační systém(y)
ÚOOÚ	Úřad pro ochranu osobních údajů (dozorový orgán pro Českou republiku)
DPO	Data Protection Officer (pověřenec pro ochranu osobních údajů), jmenovaný, popř. externí
GDPR nebo Nařízení	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
ORGANIZACE	Městský úřad Horšovský Týn a jeho organizační složky (Městská policie, Městská knihovna)

2. Definice, pojmy definice oprávněné osoby

2.1 Vymezení pojmů

Osobní údaj - Osobní údaje jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen subjekt údajů); identifikovatelnou fyzickou osobou je fyzická osoba, 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. Osobní údaje jsou jak v elektronické, tak v listinné podobě. Na obě formy se vztahují stejná pravidla zabezpečení.

Zvláštní kategorie osobních údajů (dříve Citlivý údaj) - jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace FO.

Anonymizace, Anonymizovaný osobní údaj – Anonymizovaný osobní údaj je takový údaj, který po provedené úpravě během zpracování (anonymizaci) již nelze vztáhnout k určitému nebo určitelnému subjektu údajů (např. začernění, náhrada osobních údajů jméno, příjmení iniciály apod).

Pseudonymizace - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě. Jedná se o použití „převodní tabulky“, kdy je např. zveřejněna jen tabulka obsahující pořadová čísla SÚ nebo osobní čísla zaměstnanců. Interně je ale k číslům možné přiřadit konkrétní osobu.

Zveřejněný osobní údaj - Zveřejněný osobní údaj je údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Subjekt údajů - Subjektem údajů je FO, jež své osobní údaje vlastní a pro účely zpracování je SÚ Organizaci přímo sděluje nebo je Organizace získává z jiných zdrojů. Subjektem údajů jsou jak zaměstnanci Město Horšovský Týn, tak i třetí osoby (např. dodavatelé, zaměstnanci spolupracujících organizací, představitelé a zaměstnanci orgánů státní správy a územní samosprávy, občané apod.). Subjektem osobních údajů není právnická osoba.

Zpracování osobních údajů - Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení na nosiče informací, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení

WP29 - Pracovní skupina 29 byla ustanovena článkem 29. směrnice 95/46/EC. Jde o nezávislý evropský poradní orgán na ochranu dat a soukromí složený ze zástupců dozorových orgánů. Vydává vodítka a pokyny k jednotlivým tématům GDPR.

2.2 Oprávněná osoba

Oprávněnou osobou pro účely této směrnice se rozumí osoba (zaměstnanec), určená vedoucím odboru Organizace, která v rámci své pracovní činnosti nakládá s osobními údaji, za podmínek a v rozsahu stanoveném vedoucím odboru Organizace. Činnosti zpracování, odpovědnost zaměstnanců a rozdělení kompetencí vychází z Organizačního řádu Organizace.

Zodpovědnost, kompetence

Subjekt	Zodpovědnost, kompetence
Správce – tajemník, popř. starosta Města Horšovský Týn	1. Řízení ochrany osobních údajů – určení a provádění nastavení technických a organizačních opatření ochrany OÚ, ukládání úkolů vedoucím odborů, kontrola plnění opatření 2. Zajištění realizace práv subjektů údajů (výkon realizace DPO) 3. Zodpovědnost za vypracování dokumentace GDPR (tvorba, revize, aktuálnost – Směrnice ochrany OÚ, Záznamy o činnostech zpracování, Evidence souhlasů a žádostí SÚ, Analýza rizik OÚ, Posouzení vlivu DPIA, revize Spisového a archivačního řádu) 4. Zajištění definování účelů, zákonností a prostředků zpracování OÚ pro všechny agendy zpracování OÚ v Organizaci 5. Zajištění školení a seznamování zaměstnanců Organizace s touto směrnicí, Nařízením, povinnostmi při ochraně OÚ a zajištění poskytování informací o procesech souvisejících se zpracováním OÚ

	6. Řízení rizik, určení metodiky Analýzy rizik, určení aktiv a hrozeb v Analýze rizik OÚ, verifikuje pravděpodobnost hrozby a zranitelnost všech aktiv v Analýze rizik.
Vedoucí odborů	1. Zodpovědnost za dodržování opatření stanovených touto směrnicí podřízenými zaměstnanci, zejména pak za nezpřístupnění osobních údajů zpracovávaných organizační jednotkou neoprávněným osobám (i v rámci Organizace). 2. Delegování opatření konkrétními pracovními postupy na podřízené zaměstnance 3. Určení oprávněných osob ke zpracování OÚ za svou organizační jednotku pro zpracování OÚ a přiřazení odpovídajících práv = řízení přístupů 4. Stanovení jednotlivých účelů zpracování, stanovení minimálního nutného rozsahu zpracování osobních údajů, stanovení doby uložení osobního údaje a určení zákonnosti podle příslušných agend 5. Seznámení zaměstnanců Organizace s informací o ochraně OÚ, zajištění informovanosti SÚ v oblasti poskytnutí informace a plnění práva na přístup k OÚ 6. Dohlíží na dodržování korektnosti, transparentnosti a minimálního možného zpracování osobních údajů ve vztahu k danému účelu 7. Podávání návrhů opatření a návrhů ke zlepšení procesů při zpracování a ochraně OÚ 8. Určuje míru dopadu, pravděpodobnost hrozby a posuzuje zranitelnost aktiv za svou organizační jednotku v Analýze rizik
Zaměstnanec	1. Zodpovídá za ochranu každého jednotlivého osobního údaje na svém svěřeném pracovišti a pracovním místě. Je povinen vynaložit veškeré úsilí, aby zabránil vyzrazení, pozměnění nebo ztrátě osobních údajů. A to po celou dobu zpracování nebo uložení osobních údajů na jemu svěřeném úseku. 2. Dodržuje pravidla stanovená touto směrnicí, souvisejícími interními předpisy a legislativou. 3. Neshromažďuje a nezpracovává jiné osobní údaje, než jsou pro daný účel zpracování minimálně nutné, při

	zpracování jedná maximálně transparentně a korektně 4. Ukládá nosiče dat obsahující osobní údaje na náležitě zajištěná místa a při práci s nimi postupuje tak, aby jiná osoba nemohla použít tyto nosiče jako zdroj informací, 5. Zachovává mlčenlivost o osobních údajích a o bezpečnostních opatřeních k jejich ochraně. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací, 6. Provádí průběžné ničení přípravných podkladů (rukopisů, konceptů, poznámek) sloužících ke zpracování, a to použitím odpovídajících technických a SW prostředků. 7. Oznamuje veškeré bezpečnostní události 8. Napomáhá určení míry dopadu, pravděpodobnosti hrozby a zranitelnosti aktiv v Analýze rizik
DPO (Pověřenec pro ochranu osobních údajů)	1. Konzultuje a provádí poradenskou činnost zaměstnancům Organizace 2. Vede Záznamy o činnostech zpracování 3. Vypracovává Analýzu rizik, vypočítává míru rizika, připomínkuje katalog aktiv a hrozeb (ale NEurčuje míru dopadu, pravděpodobnost hrozby a NEposuzuje zranitelnost aktiv). 4. Zajištění plnění práv SÚ, příprava odpovědí na žádosti SÚ 5. Hlášení porušení zabezpečení povinně ohlašovaných ÚOOÚ/SÚ a evidence bezpečnostních incidentů s vlivem na OÚ/SÚ

3. Dokumentace GDPR

Dokumentace související s implementací GDPR v řízené interní dokumentace Organizace:

1) Záznamy o činnostech zpracování (příloha č. 1 této Směrnice) – povinný prvek dokumentace GDPR – vymezuje:
    a. název a kontaktní údaje správce
    b. jméno a kontaktní údaje DPO
    c. účel zpracování
    d. kategorie dotčených osob (subjektů údajů)
    e. kategorie osobních údajů
    f. kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny
    g. lhůty pro výmaz (odkazem na Spisovou a archivační směrnici)

h. obecný popis technických a organizačních opatření (odkazem na Směrnici o ochraně OÚ)

2) Směrnice Ochrany osobních údajů (tato směrnice) – určuje pravidla, povinnosti a některé procesy zpracování OÚ v Organizaci včetně metodiky provádění kriteriální analýzy k DPIA a Analýze rizik OÚ
3) Směrnice DPO = kap. 14 této Směrnice, popř. smlouva s externím DPO a smlouvy o poskytnutí služeb DPO – určuje práva a povinnosti, činnost a kompetence DPO a poskytnutí služby DPO na jiné organizace

Do dokumentace GDPR dále patří:

a) vypracované Analýzy rizik,
b) záznam o přijetí rizik,
c) Posouzení vlivu na ochranu OÚ (DPIA),
d) evidence souhlasů,
e) evidence bezpečnostních incidentů a zprávy z vyhodnocení incidentů
f) smlouvy a jiné právní akty se Zpracovateli
g) Spisová a archivační směrnice určující dobu zpracování (uchování) všech dokumentů obsahujících OÚ.

Přípravu, aktualizaci a provádění změn v dokumentaci GDPR vykonává odbor kanceláře starosty, popř. DPO s vědomím a se souhlasem tajemníka, popř. starosty Města Horšovský Týn.

4. Určení pozice správce a zpracovatele, definice požadavků na zpracovatele

4.1 Správce osobních údajů

Správcem se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

Správcem osobních údajů je Organizace, resp. její tajemník, popř. starosta města.

V rámci Organizace přebírají práva a povinnosti správce osobních údajů jednotlivé odbory, zajišťující zpracovávání osobních údajů ve vymezené oblasti působnosti dle organizačního řádu.

4.2 Zpracovatel

Zpracovatel je jakýkoli externí subjekt, tedy fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatelem se rozumí subjekty, kterým správce systematicky předává OÚ za účelem dalšího zpracování nebo má k dispozici technické a organizační prostředky pro zpracování OÚ (mj. náhled).

Příkladem zpracovatele jsou dodavatelé IS, kteří mají možnost nahlížet do ostrých databází OÚ uložených v IS, příp. ukládat kopie OÚ vzdáleným přístupem na své prostředky, dodavatelé technologií, kdy dochází k ukládání OÚ přímo na prostředky zpracovatele, školitelé, právníci, účetní, marketingové agentury, kterým jsou předávány OÚ za účelem certifikace, tvorby smluv, zpracování mezd apod. Za příjemce OÚ jsou považovány organizace, kterým jsou předávány OÚ v rámci jiné povinnosti (dopravci v rámci plnění smluvního závazku – dodání zboží), předání na základě určení zákonem apod. Správce se stává zpracovatelem, pokud sám neurčil účel a prostředky, ale např. v rámci zpracování navíc zadává OÚ do IS jiného správce.

Za příjemce OÚ se nepovažují Orgány veřejné moci, kterým jsou OÚ sdělovány na základě právní povinnosti pro účely výkonu jejich úředních povinností, jako jsou daňové a celní orgány, finanční vyšetřovací jednotky, nezávislé správní orgány nebo orgány finančního trhu příslušné pro regulaci trhů

s cennými papíry a dohled nad nimi, pokud obdrží OÚ, které jsou nezbytné pro provedení konkrétního šetření. Žádost o sdělení OÚ zaslaná orgány veřejné moci by měla být vždy písemná a odůvodněná, měla by se týkat jednotlivého případu a neměla by se vztahovat na celou evidenci ani vést k propojení evidencí.

4.3 Práva a Povinnosti Správce při spolupráci se Zpracovatelem

Za Správce (Městský úřad Horšovský Týn) je pro jednání o vztahu Správce/Zpracovatel **oprávněn jednat tajemník Městského úřadu Horšovský Týn**.

Správce (Městský úřad Horšovský Týn) je povinen:

1) Subjekty Zpracovatele vybírat obzvláště pečlivě s důrazem na bezpečnost, důvěryhodnost a spolehlivost Zpracovatele. Správce prohlašuje, že vybraní Zpracovatelé poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení a při zpracování byla zajištěna odpovídající ochrana práv SÚ.
2) Uzavřít se Zpracovatelem (nebo se Správcem, pokud je Město Horšovský Týn v pozici Zpracovatele) písemnou smlouvu (dodatek smlouvy), popř. jiný právní akt podle práva Unie nebo členského státu obsahující:
    a. předmět a dobu trvání zpracování,
    b. povahu a účel zpracování,
    c. typ osobních údajů,
    d. kategorie subjektů údajů,
    e. povinnosti a práva správce,
    f. ustanovení, která Zpracovateli ukládají:
        i. zpracování OÚ pouze na základě doložených pokynů Správce
        ii. povinnost, aby se osoby Zpracovatele oprávněné zpracovávat OÚ zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
        iii. přijmutí opatření minimálně na úrovni zabezpečení zpracování dané touto směrnicí;
        iv. dodržování podmínek pro zapojení dalšího Zpracovatele, tedy, že Zpracovatel nezapojí do zpracování žádného dalšího Zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce. V případě obecného písemného povolení Zpracovatel Správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších Zpracovatelů nebo jejich nahrazení, a poskytne tak Správci příležitost vyslovit vůči těmto změnám námitky. Pokud Zpracovatel zapojí dalšího Zpracovatele, aby jménem Správce provedl určité činnosti zpracování, musí být tomuto dalšímu Zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu OÚ, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi Správcem a Zpracovatelem podle bodu 2), a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky Nařízení. Neplní-li uvedený další Zpracovatel své povinnosti v oblasti ochrany OÚ, odpovídá správci za plnění povinností dotčeného dalšího Zpracovatele i nadále plně prvotní Zpracovatel
        v. pokud to vyžaduje povaha zpracování, je Zpracovatel Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv SÚ.

vi. po ukončení poskytování služeb spojených se zpracováním v souladu s rozhodnutím Správce Zpracovatel všechny osobní údaje buď vymaže, nebo je vrátí Správci, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů.
vii. Zpracovatel Správci umožní audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověřil, a k těmto auditům přispěje.

4.4 Seznam Zpracovatelů, popř. kategorie Zpracovatelů pro Město Horšovský Týn

Kategorie zpracovatelů	***Konkrétní subjekty***
Dodavatelé IS*	Gordic, Vita Software, SW 602, Resk, Elvis, ICZ
Administrátor dotačních projektů, výběrových řízení	Domoza, ML Strategy, s.r.o.
Externí právník	AK Šůsová
Externí školitelé (BOZP, PO, povinné proškolení)	
Závodní lékař	MUDr. Luboš Kolář
Příslušné správní orgány, jiné úřady, Krajský úřad (typicky Příjemce)	
PO a organizace zřizované městem	
Dopravci	

*dodavatel IS nemusí být nutně Zpracovatel. Pokud je jeho servisní zásah jen nahodilým zpracováním OÚ postačí smluvní záruky bezpečnosti a nenakládání s OÚ, ke kterým získá dodavatel (nahodilý) přístup. Vyhodnocení míry přístupu a zpracování OÚ je třeba vždy provádět ve spolupráci IT oddělení a DPO.

5. Prostředky zpracování

Správce (Město Horšovský Týn), resp. tajemník, popř. starosta určuje prostředky zpracování OÚ v Organizaci. Určením prostředků zpracování se rozumí výběr formy zpracování:

a) Listinná podoba
b) Elektronická podoba
c) Kombinace obou forem

V případě listinné podoby určuje Správce vzory formulářů, šablony dokumentů, opatření pro ukládání, pravidla pro označování a likvidaci dokumentů a procesy oběhu dokumentů v Organizaci včetně přijetí formulářů od centrálních úřadů v oblasti přenesené působnosti.

V elektronické podobě určuje zejména konkrétní programové vybavení pro komunikaci, zápis, ukládání, čtení, zpracování výstupů a mazání osobních údajů.

Správce může prostřednictvím vedoucích určovat i detailnější prostředky zpracování, např. definici míst pro ukládání, označování dokumentů v elektronické podobě metadaty nebo názvy souborů, adresářovou strukturu, povinnost vyplňování určitých polí formuláře apod.

Každý zaměstnanec Organizace je povinen využívat pouze prostředky zpracování určené správcem, je povinen se seznámit s postupy pro jejich využití a není oprávněn využívat pro zpracování osobních údajů jiných prostředků zpracování.

V případě potřeby změn v prostředcích zpracování navrhne zaměstnanec prostřednictvím nadřízeného poradě vedoucích možnosti úpravy prostředků zpracování.

6. Stanovení účelu zpracování, zpracování OÚ

Osobní údaje se mohou v Organizaci zpracovávat pouze na základě účelů určených a zařazených do Záznamů u činnostech zpracování a na základě určení zákonného důvodu (článek 6 a článek 9 GDPR). Každý zaměstnanec Organizace se podílí na průběžné kontrole, že jsou zpracovávány pouze údaje spadající do určených účelů, osobní údaje zpracovává v souladu s příslušnou legislativou a dbá na korektnost, transparentnost a bezpečnost zpracování. V případě zjištění nedostatků okamžitě upozorní nadřízeného.

Za stanovení účelu zpracování jsou odpovědní vedoucí odboru, která danou agendu provádí dle Organizačního řádu nebo na základě určení tajemníkem, popř. starostou Organizace.

Evidenci účelů zpracování provádí DPO na základě podkladů od odborných útvarů do Záznamů o činnostech zpracování. Změny v Záznamech o činnostech zpracování dostává tajemník od DPO na vědomí.

6.1 Definice účelů zpracování

Účely zpracování vychází z jednotlivých agend, které vykonávají jednotlivé odbory. Pro sestavení Záznamů o činnostech zpracování je vhodné použít účely agregované, např. podle shodné nebo podobné legality – tedy např. právní povinnost a plnění smlouvy, naopak vyčlenit účely vyžadující souhlas. V případě právní povinnosti je vhodné vždy uvádět konkrétní legislativu.

6.2 Legalita a příklady agregovaných účelů

6.2.1 Plnění či uzavření smlouvy

Dodávka služeb, fakturace, komunikace s klientem

Nevztahuje se na marketing a vyhledávání potenciálních klientů

Uzavření pracovní smlouvy, dohody o pracovní činnosti, dohody o provedení práce a činnosti související (nábor)

6.2.2 Právní povinnost

Povinnost dle českého práva nebo práva EU

Vždy je nutné nalézt konkrétní povinnost, nejlépe včetně určení, které konkrétní údaje legislativa umožňuje zpracovávat, např.

§ Zákon o účetnictví

§ Zákoník práce

§ Zákony v oblasti soc. zabezpečení a zaměstnanosti

§ Zákon o pojišťovnictví

§ Zákon o provozu na pozemních komunikacích

§ Správní řád

§ Občanský zákoník

§ Zákon o obcích

§ Zákon o občanských průkazech,

§ Zákon o cestovních dokladech,

Příklady účelu zpracování v právní povinnosti obce:

- Evidence zemědělských podnikatelů podle zákona 252/1997 o zemědělství
- Dopravně správní agenda – registr řidičů
- Osobní doklady (občanské průkazy, pasy)
- Výkon matriční agendy
- Agenda sociálně-právní ochrany dětí

6.2.3 Oprávněný zájem

(zájmy SÚ musí převažovat nad zájmy správce); (SÚ může vznést námitku)

- Např. ochrana majetku (kamerový systém)
- Přiměřená prezentace a propagace ve školách
- Přímý marketing (v mezích legitimního očekávání)

6.2.4 Veřejný zájem či výkon veřejné moci

(SÚ může vznést námitku)

- Zpracování nezbytné pro plnění úkolů správce ve veřejném zájmu nebo při výkonu veřejné moci
- Povinnost dle českého práva nebo práva EU
- Vždy je nutné nalézt konkrétní povinnost (vhodné uvést konkrétní paragraf či článek)
- Musí být přiměřená sledovanému legitimnímu cíli
- Rozdíl oproti právní povinnosti je v tom, že se jedná o méně konkrétní úkoly, kde orgán veřejné moci nemá přímo stanovenou povinnost

6.2.5 Životně důležitý zájem

Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

6.2.6 Souhlas

Subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů, je možné jej použít pouze, pokud není možné využít jiné legality, SÚ může požádat o výmaz.

6.3 Kategorizace OÚ

V Záznamech o činnostech zpracování vede DPO údaje o kategoriích OÚ – jednotlivé OÚ rozčleněné pro stručnost a přehlednost do kategorií:

Adresní a identifikační údaje - Jméno, příjmení, adresa, datum narození, RČ, telefon, popř. e-mail a podpis přímo SÚ – nejčastější údaje vyplňované při žádostech a jednání s úřadem

Údaje o vzdělání, dosavadní praxi, odborných zkouškách – v řízení o výběru nejvhodnějšího uchazeče na úřednické místo kvůli zařazení do platové třídy/stupně

Údaje o zákonných zástupcích a rodinných příslušnících, popř. odpovědném zástupci – adresní a identifikační údaje na zákonné zástupce, rodinné příslušníky nebo osobu, která zaštiťuje podnikání svou odborností

Obrazový záznam – fotografie zpracovávané Organizací

Obrazový a zvukový záznam – videozáznam se zvukem zpracovávaný Organizací

Platební údaje – údaje o číslu účtu, bance popř. další údaje pro platební styk

Biometrické údaje – otisk prstu, podpis v agendě občanských průkazů a pasové agendě

Bytové poměry, finanční situace, údaje o rodině, zdravotní stav – v rozsahu potřebném pro posouzení situace a poskytnutí pomoci na úseku poskytování sociální péče a sociálních služeb

Projevy osobní povahy – články, kresby, malby, slohové práce apod.

6.4 Kategorizace SÚ

Zdroje OÚ jsou řazeny do kategorií pro poskytnutí relevantní informace o zpracovávání OÚ, popř. se identifikuje zdroj OÚ, pokud se nejedná přímo o SÚ.

Nejčastějšími kategoriemi SÚ v kontaktu s MěÚ Horšovský Týn jsou:

- Žadatelé, účastníci řízení, odesílatelé, adresáti, stěžovatelé, klienti, přestupci, poplatníci, jubilanti, nálezci a vlastníci, kontrolovaná osoba a jejich zákonní zástupci (občané)
- Uchazeči o zaměstnání v Organizaci
- Zaměstnanci Organizace, představitelé volených orgánů (zastupitelstvo, rada města, krizový štáb)
- Dodavatelé, Odběratelé spolupracujících organizací
- Návštěvníci akcí, města

7. Informovanost SÚ, souhlasy

Formy poskytování informací (Privacy notice):

1) Webové stránky Organizace, v patičce každého e-mailu, který odchází z Organizace, je uveden odkaz na webové stránky, část Ochrana Osobních údajů
2) Tištěná informace na podatelně
3) U vjezdu do města cedule s informací o kamerovém systému (piktogram, text, že jsou veřejná prostranství monitorovány kamerovým systémem se záznamem, kontakt na správce)

Informace je poskytována všem SÚ, jejichž OÚ Organizace zpracovává. Strukturovanou informaci pro definované kategorie SÚ připravuje a zpřístupnění informace SÚ zajišťuje odbor kancelář starosty.

Obsah Privacy notice	
Poskytnutí informace na základě čl. 13 (při získání OÚ přímo od SÚ)	**Poskytnutí informace na základě čl. 14 (při získání OÚ jiným způsobem než přímo od SÚ)**
a) totožnost a kontaktní údaje správce a jeho případného zástupce **c) účely zpracování, pro které jsou osobní údaje určeny** **d) právní základ pro zpracování (zákonnost)** **e) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na zákonném důvodu "oprávněný zájem"** f) případné příjemce nebo kategorie příjemců osobních údajů g) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci ***Důležité!*** ***pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) = na SOUHLASU SÚ, je SÚ v informaci vždy upozorněn na existenci práva odvolat kdykoli souhlas, aniž by tím byla dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;*** ***pokud je zpracování založeno na základě čl. 6 odst. 1 písm. f) = OPRÁVNĚNÉM ZÁJMU, včetně profilování založeného na těchto ustanoveních je Subjekt údajů upozorněn na právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, V případě podání námitky Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.*** v případě získání údajů od SÚ, v případě potřeby a pro snížení rizika se poskytují dále ještě následující informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování: a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;	a) totožnost a kontaktní údaje správce a případně jeho zástupce b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů c) účely zpracování, pro které jsou osobní údaje určeny d) právní základ pro zpracování **e) kategorie dotčených osobních údajů** f) případné příjemce nebo kategorie příjemců osobních údajů g) případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci

b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, jakož i práva na přenositelnost údajů;	
d) existence práva podat stížnost u dozorového úřadu;	
e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;	
f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.	

V souladu s určením účelu na odborných útvarech je stanovena i povinnost určit zákonnost daného účelu zpracování. V případě nejasností je možná konzultace DPO a/nebo právního poradce. V případě, že je zákonnou povinností SOUHLAS se zpracováním OÚ, tedy není možný jiný zákonný důvod a zpracování je i tak nezbytné pro potřeby a naplnění cílů organizace, je třeba **před zahájením zpracování** opatřit souhlasy dotčených SÚ.

1) Souhlas musí být:
    a. Svobodný a odvolatelný
    b. Určitý
    c. Informovaný
    d. Srozumitelný
    e. Jednoznačný
    f. Strukturovaný, tedy pro každou část možnost vyjádření zvlášť
2) Pokud je zpracování založeno na souhlasu, musí být Organizace schopna doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů = vedení evidence souhlasů
3) Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.
4) Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

5) Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.

Souhlas je možné dát písemně nebo službou informační společnosti, případně tzv. konkludentním způsobem, kdy musí být např. návštěvníci akce upozorněni na možnost pořizování fotografií a způsob jejich prezentace např. v pozvánce, na cedulích v areálu, při registraci apod. (navíc oproti standardní Privacy notice informaci). Současně jim musí být poskytnuty informace, že mohou fotografování odmítnout a informace jakým způsobem mohou svůj (konkludentní) souhlas odvolat. Organizace musí rovněž po celou dobu zpracování souhlasy evidovat, aby byla schopna udělení souhlasu kdykoliv doložit (v případě konkludentního souhlasu např. dokumentací obsahu a umístění informačních tabulí).

Textaci souhlasu připraví odborné útvary ve spolupráci s DPO, popř. právníkem, za získání souhlasů jsou odpovědní vedoucí odborů, které zpracování (agendu) zajišťují.

Písemné souhlasy jsou vedeny

a) ve spisu, který je veden pro daný účel zpracování spolu s dalšími dokumenty, nebo
b) spolu s dalšími souhlasy potřebnými pro daný účel zpracování

Dokumenty prokazující použití konkludentního souhlasu jsou uchovány v rámci dokumentace konkrétní akce.

Souhlas udělený službou informační společnosti je pouze evidován v evidenci souhlasů.

Odvolání souhlasu mohou SÚ podat na kterémkoliv odboru nebo podatelně a to způsobem, jakým souhlas se zpracováním udělily. **Při odvolání souhlasu je vhodné aplikovat přiměřené ověření totožnosti odvolatele.**

7.1 Vedení evidence souhlasů

Podatelna vede centrální evidenci souhlasů za všechny organizační jednotky (Organizace). Udělení nebo odvolání souhlasu s konkrétním zpracováním OÚ hlásí vedoucí odborů nebo jimi pověřené osoby na podatelnu.

8. Likvidace osobních údajů

Pro zpracování každého osobního údaje je stanoven účel, minimální rozsah a doba uložení (zpracování) osobních údajů (jak v listinné, tak v elektronické podobě). Doba uložení a proces vyřazení dokumentů je stanoven Spisovým a archivačním řádem, který zohledňuje lhůty dané legislativou a je průběžně aktualizován.

8.1 Likvidace osobních údajů v elektronické podobě

1. Osobní údaje jsou mazány prostředky operačního systému daného počítače.

2. Paměťová zálohovací média nebo paměťová přenosná média musí být v případě vyřazení opakovaně přepsána a následně nízko úrovňově přeformátována nebo fyzicky zničena.

3. Paměťová média počítačů musí být v případě jejich vyřazení opakovaně přepsána a následně nízko úrovňově přeformátována nebo fyzicky zničena.

Likvidaci podle spisového a archivačního řádu zajišťují zaměstnanci odborných útvarů, formátování, fyzickou likvidaci nosičů zajišťuje oddělení IT.

8.2 Likvidace osobních údajů v listinné podobě

1. Osobní údaje v listinné podobě jsou ničeny pomocí skartovacího zařízení. Skartace probíhá dle spisového a archivačního řádu. O skartaci dokumentu je proveden záznam např. tabulkou skartovaných dokumentů z důvodu prokázání likvidace OÚ po vypršení lhůty zpracování. V případě zapojení externího subjektu jsou dodrženy pravidla pro výběr zpracovatele dle kap. 3 s důrazem na spolehlivost dodavatele a vždy je požadováno doložení skartace z důvodu prokázání likvidace dokumentů.

9. Metodika AR, frekvence opakování AR, hodnocení výstupů z AR

Analýza rizik se provádí zpravidla 1x za 2 roky, případně dle potřeby při změně účelů zpracování OÚ (aktiv) nebo změně hrozeb, případně při zavádění nových činností Organizace.

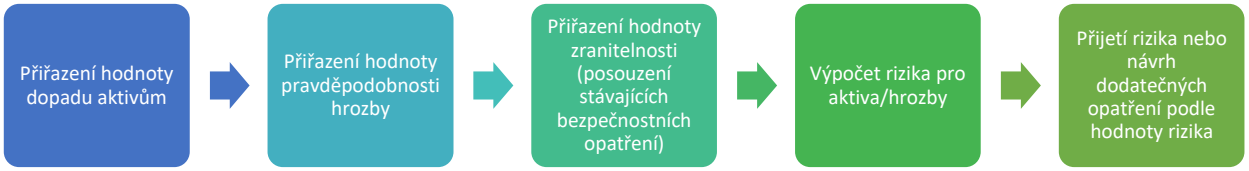
Analýzu rizik (určení dopadů a pravděpodobnost hrozeb) připravuje písemně DPO ve spolupráci s odbornými útvary, zodpovědnost za vedení a aktuálnost řízené interní dokumentace GDPR obecně má správce (tajemník, popř. starosta města). DPO dále navrhuje opatření ke zmírnění rizik, jejich realizace je pak v kompetenci tajemníka a vedoucích odborů MěÚ Horšovský Týn. Organizace provádí Analýzu rizik podle metodiky, viz níže.

DPO pravidelně kontroluje a reviduje aktiva, hrozby a používanou metodiku.

9.1 Metodika analýzy rizik

Postup zpracování analýzy rizik je dán níže uvedeným diagramem a má následující fáze:

1) Identifikace aktiv, posouzení dopadu
2) Určení hrozeb aktivům a jejich ohodnocení
3) Posouzení bezpečnostních opatření a přiřazení hodnoty zranitelnosti
4) Výpočet rizika
5) Návrh dodatečných opatření podle hodnoty rizika



9.2 Aktiva

Hodnota aktiva bude určena pro každý účel zpracování posouzením dopadu, která SÚ hrozí v případě, že by došlo k naplnění hrozby. Hodnotí se:

Potenciální újma SÚ	***Vysvětlení***
Reputační škoda	Poškození jména, snížení uplatnění atd.
Zneužití identity	Možná krádež identity
Obtěžování	Využití třetí stranou pro nevyžádanou nabídku produktů/služeb, využití jako nástroj šikany apod.
Ztráta soukromí	Vyzrazení bydliště, telefonního čísla atd.

Hodnota dopadu se stanoví pro každou ze čtyř možností újmy, která by byla způsobena subjektu OÚ v případě úniku, zneužití, zcizení OÚ (Reputační škoda, Zneužití identity, Obtěžování, Ztráta soukromí). **Hodnotitelem jsou vedoucí odboru za svou organizační jednotku.**

1	Nízký	Nemá vliv na život subjektu
2	Střední	Limituje subjekt
3	Vysoký	Vyžaduje změny chování a jednání subjektu

Celková hodnota aktiva hodnocením dopadu je vypočtena jako aritmetický průměr z hodnot dopadu pro každou možnost potenciální újmy subjektu údajů:

Hodnota aktiva = Dopad (Reputační škoda * Zneužití identity * Obtěžování * Ztráta soukromí)/4

Výsledná hodnota aktiva nabývá hodnot v krocích po 0,25 od **1,00 do 3,00**.

9.3 Hrozba

Definice hrozby: hrozba je potenciální příčina bezpečnostní události nebo bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.

Hrozba	***Popis hrozby***
Lidská chyba - neúmyslná (z nepozornosti, nedbalosti, neznalosti)	K poškození práv a svobod SÚ dojde neúmyslně při činnosti zpracování nebo při podpůrných činnostech.
Zneužití OÚ oprávněnými osobami	Dojde ke zneužití informací uložených v listinné nebo elektronické podobě, OÚ jsou použity k jinému než povolenému účelu nebo jiným způsobem než popisuje tato směrnice/legislativa.
Neoprávněný přístup, únik informací z nosičů – listinná podoba	OÚ v listinné podobě jsou zpřístupněny osobám, které k tomu nebyly oprávněny (systémová chyba=chybné nastavení přístupu, nahodilá událost=odemčená kancelář, dokumenty na stole jsou přístupné i cizím osobám, jsou zveřejněny seznamy OÚ bez legálního účelu zpracování).
Neoprávněný přístup, únik informací z nosičů – elektronická podoba	OÚ v elektronické podobě jsou zpřístupněny osobám, které k tomu nebyly oprávněny (systémová chyba=chybné nastavení přístupových práv, nahodilá událost=únik přístupových údajů, odeslání seznamu OÚ e-mailem na nesprávnou adresu, zveřejnění OÚ na webových stránkách bez legálního účelu zpracování, zaměstnanec zkopíruje databázi zákazníků na USB flash a prodá jí konkurenci.).
Porušení zákonných předpisů	Při zpracování jsou porušeny zásady korektnosti, transparentnosti a bezpečnosti nebo přímé postupy dané legislativou/pracovními postupy.
Živelní událost (požár, voda, ostatní) - fyzické poškození nebo zničení OÚ nebo technických nosičů, havárie technických prostředků	Událost, při které dojde ke ztrátě nebo zničení (např. požár, povodeň), havárie technický prostředků. Bez ohledu na formu zpracování (listinná nebo elektronická)
Kybernetická hrozba - útok zvenčí	Dos, DDos útok, útok ransomware, šifrování, trojské koně, malware, phishing, tabnabbing apod.

Hodnotitel hodnotí pravděpodobnost hrozby pro každé aktivum (účel zpracování). **Hodnotitelem jsou vedoucí odboru za svou organizační jednotku.**

Stupnice hodnocení pravděpodobnosti hrozby

Body	***Pravděpodobnost***	***Definice pravděpodobnosti***
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za rok.
3	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
5	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je kratší než 1 měsíc.

9.4 Zranitelnost

Definice zranitelnosti: zranitelností je slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami. **Hodnotitelem jsou vedoucí odboru za svou organizační jednotku.** Hodnotitel určuje míru zranitelnosti na stupnici 1-4:

1	Nízká	Zranitelnost je málo pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována
2	Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost podléhá kontrolním mechanismům. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezená. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření

9.5 Riziko

Pro každý účel zpracování (aktivum) a hrozbu je stanoveno riziko podle vzorce: **riziko = celková hodnota aktiva x zranitelnost x hrozba. Riziko každého účelu (aktiva) může dosahovat hodnot v rozmezí 1,00 až 60.**

Stupeň rizika (počet bodů)	Od	Do	Opatření
nízká	1	5,99	Opatření jsou dostatečná
střední	6	18,99	Opatření je třeba revidovat, riziko je možné přijmout (vedoucí odboru)
vysoká	19	44,99	Opatření je třeba neprodleně revidovat, riziko je možné přijmout písemně vedením Organizace
kritická	45	60	Riziko není možné přijmout, je nutné přijmout další opatření, popř. konzultovat s ÚOOÚ

Výpočet rizika, představení výsledku Analýzy rizik vedení Organizace a návrhy opatření pro snížení rizika provádí DPO.

Cílem hodnocení rizik je:

- prokázat, že navržená bezpečnostní opatření jsou dostatečná,
- identifikovat případnou potřebu realizace dodatečných bezpečnostních opatření.

9.6 Vypořádání se s riziky

Povinností Organizace je projednat výstupy z analýzy rizik a rozhodnout o dalším postupu ve vypořádání rizik, které může být následující:

- akceptace zvýšeného rizika (úroveň střední-vysoká) zejména z důvodu ekonomické neúnosnosti protiopatření;
- akceptaci středních rizik může učinit samostatně i vedoucí odboru s vědomím vedení
- akceptaci vysokých rizik musí rozhodnout porada vedení
- rozhodnutí o vyhnutí se riziku:
    - neprovádění určitých aktivit (např. může být rozhodnuto, že IS nebude zpracovávat určité údaje nebo bude omezen přístup k nim);
    - přemístěním aktiv mimo oblast rizika;
- rozhodnutí o přenesení rizika na třetí stranu (dodavatel, pojišťovna, …);
- přeskupení aktiv tak, aby se snížila jejich hodnota (např. rozložení informací na více míst apod.), uvolnění dalších zdrojů pro řešení rizik a přijetí opatření, které eliminuje riziko.

10. Ochrana osobních údajů

10.1 Nutnost ochrany OÚ

Osobní údaje jsou vlastnictvím Subjektů údajů, a proto je třeba při jakémkoli zpracování dodržovat nejen pravidla zákonnosti, korektnosti a transparentnosti, ale je nutné je také odpovídajícím způsobem chránit zejména před náhodným nebo protiprávním zničením, ztrátou, pozměňováním, neoprávněným zpřístupněním předávaných, uložených nebo jinak zpracovávaných OÚ, nebo neoprávněný přístup k nim. Riziko škody/újmy SÚ zohledňuje Správce prováděním Analýzy rizik.

Na základě výsledků Analýzy rizik s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování určuje Správce technická a organizační opatření touto směrnicí, aby zajistil úroveň zabezpečení odpovídající danému riziku, zejména pak zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování a schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.

10.2 Organizační opatření

Organizace zajistila obecné proškolení všech zaměstnanců prokazatelným způsobem s GDPR k 25. 5. 2018. Organizace zajistí proškolení v případě změn legislativy a promítnutí legislativních změn do interních předpisů. Školení je zaměřeno zejména na povinnosti organizace, povinnosti zaměstnanců, jejich odpovědnost a principy ochrany osobních údajů.

Vedoucí zaměstnanci dbají na aplikaci principů ochrany osobních údajů a transparentního a korektního zpracování při zpracování OÚ zaměstnanci.

Organizace zajišťuje proškolení nových zaměstnanců s principy GDPR a ochrany osobních údajů prostřednictvím této Směrnice. Seznámení se směrnicí a základní informací o zpracování osobních údajů zaměstnanců je součástí úvodního zaškolení zaměstnance.

Organizace zajistí dodatečné odborné školení oprávněných osob na základě zařazení školení do plánu odborných školení, na základě výsledků Analýzy rizik nebo výsledků kontrol nastavených opatření a případně na základě vyhodnocení bezpečnostních incidentů.

Organizace zajišťuje kompetence a procesy pro zajištění informovanosti SÚ, plnění práv SÚ a ochrany OÚ prostřednictvím této směrnice.

Organizace zajišťuje specifická školení v oblasti kybernetické bezpečnosti a trendech v informatice v rámci odborného vzdělávání pracovníků IT.

10.3 Řízení přístupů

1. Instalaci na stanice a přístupová oprávnění do jednotlivých IS přidělují vedoucí jednotlivých odborů, nastavení provádí IT.

2. Účty do centrálního IS a do dílčích IS jsou řazeny do skupin podle potřeby přístupu k údajům, datům a možnosti editace.

3. Oddělení IT sestavuje a aktualizuje seznam skupin a jim odpovídajících práv a v případě potřeby identifikuje uživatele přiřazené do těchto skupin.

4. Správu skupin (agendových IS), jim přiřazených práv a přiřazení jednotlivých uživatelů do skupin (nebo přístupy do agendových IS) provádí IT pouze v případě:

    a. Nástupu nového zaměstnance podle informací o pracovním zařazení
    b. Změny v přístupech s potvrzením vedoucího odboru, ze kterého je zaměstnanec a případně vedoucího odboru, v jehož kompetenci jsou data/aplikace, kam je požadavek směřován

Změny ve struktuře skupin/změny v agendových IS provádí IT pouze s potvrzením dotčených vedoucích odborů a tajemníka MěÚ Horšovský Týn.

10.4 Ochrana osobních údajů v elektronické podobě

1. IS provozované Organizací (blíže viz kapitola „Prostředky zpracování“) jsou chráněny před působením škodlivého kódu nasazením antivirového systému. Provozovaný antivirový systém se minimálně 1x denně aktualizuje. Není-li možné napadený soubor s osobními údaji „vyléčit“, je přesunut do karantény. O dalším postupu v takovém případě rozhodne vedoucí IT. Antivirový systém musí mít aktivovánu rezidentní část, která zajišťuje online kontrolu otevíraných souborů.

2. Antivirový systém vytváří záznamy o infikovaných souborech, o infikovaných počítačích, o akci, která byla antivirovým systémem provedena, o typu infekce. K záznamům mají přístup pracovníci IT.

3. Vnitřní síť ORGANIZACE je oddělena od veřejných sítí firewallem. Firewall má povoleny služby a porty nutné pro fungování provozovaných aplikací, vše ostatní je uzavřeno. O otevření portu a služeb rozhoduje vedoucí IT. Firewall musí odolat DoS a DDoS útokům.

4. Firewall vytváří záznamy o útocích, o zdrojích útoků, o akci, která byla firewallem provedena. K záznamům mají přístup pracovníci IT.

5. Přístup k síti ORGANIZACE a jejím zdrojům a k osobním údajům je možný jen na základě úspěšné autentizace do domény. Pro autentizaci je používána kombinace uživatelského jména a hesla. Heslo musí být minimálně 8 znaků dlouhé, musí kombinovat velká a malá písmena, číslice a speciální znaky. Heslo je měněno minimálně 1x za 6 měsíců. Po 3 neúspěšných pokusech je účet zablokován. Odblokovat účet je oprávněn pracovník IT.

6. Na stanicích a mobilních zařízeních je nastaven časový interval, po kterém dojde k zamčení (stanice/displeje). Interval nesmí být kratší než 30minut.

7. Všichni uživatelé jsou při zřízení uživatelských účtů poučení o povinnosti striktního zákazu sdělování přístupových údajů dalším osobám nebo jejich uchování nezabezpečeným způsobem (lístečky na stole, nástěnce, monitoru, na/v telefonu/mobilním zařízení) apod.

8. Doména vytváří záznamy o přihlášení a o neúspěšných pokusech o přihlášení. K záznamům mají přístup pracovníci IT.

9. Přístup k aplikacím a jejich zdrojům a k osobním údajům je možný jen na základě úspěšné autentizace. Část aplikací přebírá autentizaci z domény, část provádí autentizaci vlastními prostředky (vždy je nastaveno nejsilnější možné heslo).

10. Aplikace vytváří záznamy o přihlášení, o neúspěšných pokusech o přihlášení a o operacích s daty v rámci aplikace do rozsahu, jaký každá jednotlivá aplikace umožňuje. K záznamům mají přístup pracovníci IT.

11. Data a osobní údaje jsou zálohovány. Zálohování je prováděno zálohovacím systémem, který nastavují pracovníci IT.

12. Zálohovací systém vytváří záznamy o zálohovacích operacích. K záznamům mají přístup pracovníci IT.

13. Dostupnost dat uložených na centrálních úložištích je dále zvýšena použitím UPS a dieselagregátu pro případ výpadku elektrického proudu.

14. Osobní údaje Zvláštní kategorie osobních údajů jsou v elektronické podobě chráněny stejným způsobem jako osobní údaje ostatní.

15. Uživatelé PC stanic ukládají data primárně na zálohovaná síťová úložiště k tomu určená. Na lokální počítače jsou ukládána zejména data dočasná, pracovní apod. s vědomím, že nedochází k jejich záloze – a tudíž může dojít k jejich ztrátě. Osobní údaje zaměstnanců a citlivé údaje občanů nejsou ukládány na lokální disky nikdy.

16. Displeje počítačů musí být otočeny tak, aby v případě návštěvy kanceláře třetí stranou neměla třetí strana možnost odečíst osobní údaje.

17. Stanicím v doméně je zakázáno použití zápisu prostřednictvím CD/DVD mechanik mimo výjimečných případů nutných pro splnění pracovní agendy.

18. Uživatelé nesmí používat USB flash zařízení v Organizaci pro uchovávání dat. Výjimkou je krátkodobé uložení dat na USB flash pro přenos dat mezi stanicemi v rámci Organizace.

19. Je zakázáno vynášet na jakémkoli zařízení data Organizace. Výjimku tvoří zaměstnanci s přidělenými služebními notebooky (NTB) a zaměstnanci, kteří mohou pracovat mimo areál Organizace (Home office).

20. Data na NTB se primárně neukládají (využití síťových úložišť). Pokud jsou na NTB uloženy osobní údaje, je uložen na oddílu, který je chráněn šifrováním (např. BitLocker).

21. Správci IS ORGANIZACE jsou povinni se přihlašovat svými jmennými účty, které mají odpovídající práva pro správu systémů. Činnost správců je zaznamenávána doménou a aplikacemi stejně jako je tomu u běžných uživatelů. Přístup k záznamům je omezen na správce, záznamy jsou chráněny před neoprávněným přístupem a manipulací, jsou zálohovány po dobu 3 měsíců.

10.5 Ochrana osobních údajů v listinné podobě

1. Osobní údaje v listinné podobě jsou uchovávány v uzamčených místnostech. Není možné, aby měla k osobním údajům přístup neoprávněná osoba. V pracovní době není možný přístup na jednotlivá pracoviště v nepřítomnosti odpovídajícího pracovníka. Úklid kancelářských prostor je prováděn v pracovní době a za přítomnosti oprávněných osob v kanceláři.

2. Listiny s osobními údaji Zvláštní kategorie osobních údajů musí být mimo pracovní dobu umístěny v zamykatelném šuplíku nebo skříni.

3. V případě návštěvy kanceláře třetí stranou musí být listiny s osobními údaji uloženy takovým způsobem, že třetí strana nebude mít možnost osobní údaje odečíst.

4. Při přenášení listin obsahujících osobní údaje je nutné věnovat této činnosti zvýšenou pozornost tak, aby nedošlo ke ztrátě takových listin nebo zpřístupnění OÚ neoprávněným osobám.

5. V případě, že přeprava dokumentů obsahující osobní údaje je svěřena jiným, k tomu určeným subjektům, je oprávněná osoba povinna tyto dokumenty umístit samostatně podle jednotlivých adresátů v uzavřených obalech (např. zalepená obálka nebo krabice s přelepem a signaturou či razítkem).

6. Dokumenty se zvýšeným rizikem narušení soukromí nebo svobod SÚ nebo s vyšší hodnotou pro Organizaci jsou vždy chráněny dalšími prvky objektové bezpečnosti – elektronickým zabezpečovacím zařízením, popř. mřížemi a zvýšenou ochranou proti požáru (EPS).

10.6 Bezpečnostní desatero

ORGANIZACE dbá na bezpečnost osobních údajů, dat a informací. Všechna bezpečnostní opatření a bezpečnostní mechanismy jsou však neúčinné pokud není dodržován elementární bezpečnostní přístup uživatelů informačního systému.

V této souvislosti je níže uvedeno několik **základních pravidel, které je potřeba mít neustále na paměti**.

1. Při jakkoli krátkém opuštění svého pracovního místa je **nutné** zamknout pracovní stanici (zkratka Win+L, odhlášení);
2. Při jakkoli krátkém opuštění svého pracovního místa je třeba **veškeré** materiály, které svým charakterem obsahuji **citlivé informace** (osobní údaje, interní informace, apod.) alespoň uložit do zásuvky – tzv. zásada čistého pracovního stolu; **obzvláště to platí pro ty, kteří přicházejí v kanceláři ke styku s třetími stranami** (zákazníci, dodavatelé, uchazeči o zaměstnání atp.);
3. Při pořizování kopií a skenování je potřeba se přesvědčit, zda v kopírce/skeneru nezůstal originál dokumentu;
4. Při tisku dokumentů, které svým charakter odpovídají citlivé informaci, je potřeba si tisk **okamžitě** vyzvednout u tiskárny, a to v případě tisku na sdílené stroje. Je potřeba mít přitom na zřeteli i dokumenty, které se „zaseknou" v tiskové frontě a mohly by se vytisknout „samy" později. Stejně tak je potřeba se přesvědčit, zda netisknete náhodou na jinou než zamýšlenou tiskárnu;
5. V případě elektronické komunikace, zkontrolujte adresáta emailu, aby zpráva nebyla omylem odeslána nezamýšlené osobě. Nepřeposílejte obsah komunikace s třetí osobou a pokud to není nutné, nepoužívejte volbu „odpovědět všem" – Reply to all.
6. **Citlivé informace je povoleno ukládat jen na zabezpečená interní datová uložiště**. Je zakázáno ukládat citlivá a nezabezpečená data (šifrováním nebo dostatečně silným heslem) na cloudová uložiště (DropBox, SkyDrive, uloz.to, uschovna.cz apod.);
7. **Při práci s elektronickou poštou je potřeba být obezřetný** a dostatečně rezistentní vůči emailům s podvodným a potencionálně nebezpečným obsahem. Neotevírat a **neklikat v emailu na odkazy a neotevírat přílohy**, pokud není jistota pravosti obsahu – věrohodný odesilatel, informace v emailu a případně adresy uvedených odkazů. **Nezapomeňte na to, že email je snadné zfalšovat a podvrhnout**;
8. Na prostředcích ORGANIZACE a na všech prostředcích, které jsou připojeny do sítě ORGANIZACE, **není dovoleno navštěvovat internetové stránky** s potenciálně nebezpečným obsahem (erotické stránky, „warez" stránky apod.) a **taktéž z internetu stahovat obsah, který nesouvisí s pracovní činností** (jakýkoliv software). **Svěřené pracovní prostředky nejsou určeny k soukromým účelům**. Uživatelům je zakázáno v IT prostředí Organizace používání vlastních paměťových médií (diskety, CD a DVD, USB paměti, atp.);
9. Je potřeba kontrolovat a zavírat za sebou vstupní dveře, které oddělují veřejně dostupné prostory od interních a **být obezřetný ke komukoli, koho neznáte**. Ti, kteří mají přístup do serveroven a jiných neveřejných prostor, se před odchodem musí přesvědčit, že za sebou nenechali otevřené a nezamčené dveře;
10. Stejně jako čistý stůl je třeba udržovat i pracovní plochu počítače „čistou". Na plochu patří pouze zástupci často potřebných souborů, složek či aplikací.

11. Kriteriální analýza k DPIA

DPO spolupracuje s osobou pověřenou zpracováním Posouzení vlivu za Organizaci na vypracování kriteriální analýzy, jestli je nutné vypracování formálního Posouzení vlivu na soukromí subjektů údajů. DPO má roli poradní, konzultační a metodickou.

Kriteriální analýza je třeba provést vždy, když je do Záznamů o činnostech zpracování přidán nový účel zpracování nebo se výrazným způsobem změní prostředky zpracování stávajícího účelu. O přidání/změně účelu je informován DPO vedoucími odborů. O výsledku kriteriální analýzy je DPO informován osobou pověřenou jejím vypracováním.

DPIA nebude nikdy provedeno pro agendy, kdy se jedná o činnosti v přenesené působnosti státu.

O provedení kriteriální analýzy, zda je nutné provést formální posouzení vlivu je DPO proveden záznam do tabulky Záznamy o činnostech zpracování – zápis hodnoty výsledku kriteriální analýzy.

Kritéria posouzení:

kritérium 1 - určení míry monitorování subjektů údajů	
	Subjekty údajů jsou identifikovatelné/identifikované a lokalizovatelné
	(Poznámka: Jedná se zejména o zpracování údajů monitorujících pohyb identifikovatelných subjektů údajů).
	Subjekty údajů jsou identifikovatelné/identifikované a rozpoznatelné
	(Poznámka: Jedná se zejména o zpracování obrazových záznamů identifikovatelných subjektů údajů).
	Subjekty údajů jsou identifikovatelné/identifikované
kritérium 2 - údaje shromažďované o subjektech údajů	
	zvláštní kategorie údajů a údaje týkající se rozsudků ve věcech trestních a trestných činů
	(Poznámka: Zpracování zahrnuje vedení osobních údajů o rasovém nebo etnickém původu, o politických názorech, o náboženském vyznání, o filozofickém přesvědčení, o členství v odborech, o zdravotním stavu, o sexuálním životě a sexuální orientaci fyzické osoby, genetické údaje, biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje týkající se rozsudků ve věcech trestních a trestných činů a apod.).
	provozní a další údaje využitelné pro vytváření profilů uživatelů nebo automatizovaného rozhodování
	(Poznámka: Například údaje z logů, historie navštívených stránek, údaje o uskutečněných voláních, údaje elektronické pošty, údaje o zařízeních (např. ICT) používaných subjektem údajů, finanční údaje (zahrnuje údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách, platební morálce) apod.).
	údaje umožňující vystupovat/jednat jménem subjektu údajů v souvislostech znamenajících poškození cti, pověsti, charakteru, bezúhonnosti
	(Poznámka: Zpracování zahrnuje zpracování údajů přístupové jméno, heslo/PIN, role, pseudonym, přestupky, pokuty, účast na některých akcích apod.).
	údaje umožňující na účet subjekt údajů odbírat služby, zboží, vybírat peníze
	(Poznámka: Zpracování zahrnuje údaje jméno subjektu (společně jméno a příjmení), datum narození, číslo platební karty, heslo/PIN, zákaznické číslo, telefonní číslo, e-mailová adresa, adresa pobytu vlastnictví nemovitostí, vlastnictví dopravních prostředků apod.).
	jedinečné identifikační údaje
	(Poznámka: Zpracování zahrnuje údaje jméno subjektu (společně jméno, příjmení, tituly, datum narození), RČ, číslo sociálního pojištění, číslo zdravotního pojištění, číslo OP, číslo pasu, číslo ŘP, AIFO apod.).
	údaje spojené s chováním subjektu údajů

	(Poznámka. Zpracování zahrnuje zpracování údajů účast na některých akcích, vzdělávání, popis praxe, zájmy, údaje o členství apod.).
	ostatní osobní údaje, včetně některých zvláštních případů
	(Poznámka. Zpracování zahrnuje údaje softbiometrické údaje (jako je váha, výška, konfekční velikosti, barva vlasů, barva očí, pohlaví, věk apod.), prosté obrazové záznamy, identifikátory subjektů, které nejsou jedinečné, údaje o nákupech apod.).
kritérium 3 - rozsah zpracování osobních údajů	
	velký rozsah zpracování osobních údajů
	(Poznámka: od 10001 subjektů údajů a/nebo nad 20 přistupujících osob)
	střední rozsah zpracování osobních údajů
	(Poznámka: od 5001 do 10000 subjektů údajů a/nebo od 3 do 20 přistupujících osob)
	malý rozsah zpracování osobních údajů
	(Poznámka: do 5000 subjektů údajů a/nebo do 2 přistupujících osob k osobním údajům).
kritérium 4 - vazby na jiné subjekty	
	s vazbami na nejednoznačně vymezené správce
	(Poznámka: Vazba je dána například jen kategorií správce například orgány veřejné správy, nemocnice, školy, členové podnikatelských seskupení, a to proto, že seznam není možno vyčerpávajícím způsobem určit nebo je proměnlivý apod.)
	s vazbami na jednoznačně vymezené správce/zpracovatele
	(Poznámka: Lze uvést vyčerpávající seznam správců a/nebo zpracovatelů)
	bez vazeb na jiné správce /zpracovatele
kritérium 5 - inovativnost řešení	
	zcela nové řešení (dosud nerealizované zpracování osobních údajů)
	(Poznámka: Jedná se pro správce nebo zpracovatele o nová řešení, nikde dosud na území ČR nerealizovaná, se kterými nejsou žádné zkušenosti).
	první nasazení řešení (již známého zpracování osobních údajů) u správce nebo zpracovatele
	(Poznámka: Jedná se pro správce nebo zpracovatele o nové řešení, ale správce nebo zpracovatel může využít zkušeností jiného člena konsorcia nebo jiného subjektu na území ČR (například dodavatele).
	obdobné řešení u správce již nasazené nebo prvně nasazené u správce, ale jde o opakované řešení (nabízené na trhu dodavatelem se škálovatelným nastavením)
	(Poznámka Jedná se o řešení, se kterými má správce již zkušenosti nebo řešení mnohokrát různě nasazená a odzkoušená „krabicová řešení“ nebo „řešení na klíč“ dodávaná a přizpůsobitelná dle potřeb správce).
kritérium 6 - k zasaženému území z hlediska subjektů údajů	
	podrobná úroveň - místa veřejně přístupná

	(Poznámka: Týká se rozsahu menšího než obec – veřejná prostranství, pasáže apod. - míří na kamerové systémy monitorující ve velkém rozsahu veřejná prostranství).
	podrobná úroveň - místa veřejně omezeně přístupná nebo nepřístupná
	(Poznámka: Týká se rozsahu menšího než obec - pozemky majitele, interiéry objektů jako bytové domy, průmyslové objekty, prodejny a také velmi omezeně (1-1,5m) veřejná prostranství, těsně přilehlá k monitorovanému subjektu - míří na kamerové systémy).
	lokální úroveň- do území regionu
	(Poznámka: Jedná se o jednotky LAU2 (NUTS5)=obce, LAU1 (dříveNUTS4)=okresy, NUTS3=kraje apod.).
	regionální úroveň - území regionu
	(Poznámka: Jedná se o jednotky (NUTS2=region).
	národní úroveň - území země nebo státu
	(Poznámka: Jedná se o jednotky (NUTS0=stát, NUTS1=země).
	nadnárodní úroveň
	(Poznámka: Jedná se o jednotky na úrovni skupiny zemí).

Za každé kritérium se přidělí body podle rizika-ohrožení SÚ

nízká	1
střední	3
vysoká	5

Body za všechna kritéria se sečtou.

Možná škála sečtených bodů

Stupeň rizika (počet bodů)	Od	Do
nízká	6	15
střední	16	22
vysoká	23	30

Formální posouzení vlivu se provede v případě, že z kriteriální analýzy DPIA vyšlo vysoké riziko (rozmezí bodů 23-30).

- Minimální náležitosti posouzení vlivu na ochranu osobních údajů (článek 35, odst. 7):
  - systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;
  - posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
  - posouzení rizik pro práva a svobody subjektů údajů

– plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob

Provedením posouzení vlivu se reálně posoudí rizika a opatření. Tím, že z kriteriální analýzy vzešlo zvýšené riziko, je vhodné přidat pro daný účel zpracování opatření ke snížení rizika pro práva a svobody SÚ. V případě, že i po zavedení dodatečného opatření zůstává riziko pro práva osob vysoké, je třeba konzultace s ÚOOÚ.

Návrh opatření a konzultaci s ÚOOÚ zajistí ve spolupráci osoba pověřená provedením Posouzení vlivu a DPO.

12. Žádosti Subjektů údajů

Žádosti Subjektů údajů mohou mít různou povahu i formu. Žadateli není nikdy odpovídáno bez řádné autentizace Žadatele. Odpověď Žadateli připraví DPO a odešle odbor kancelář starosty (podpis tajemníka, starosty, datová schránka).

Žádost o plnění práva SÚ podává žadatel zpravidla:

1. ústně, tj osobní návštěvou Organizace
2. písemně, a to i prostřednictvím sítě nebo služby elektronických komunikací (e-mail podepsaný elektronickým podpisem, datová schránka)

Telefonické žádosti se neevidují a neodpovídá se na ně z důvodu nemožnosti autentizace osoby žadatele. Žadatel je odkázán na písemnou formu žádosti nebo osobní kontakt v Organizaci. U žádostí doručené prostým e-mailem je postupováno stejně, žadatel je odkázán na jinou formu podání z důvodu nemožnosti autentizace SÚ.

Telefonicky nebo prostým e-mailem se nikdy nesdělují jakékoliv osobní údaje zaměstnanců nebo osobní údaje podléhající mlčenlivosti osobám, které jsou žadateli o práva subjektů údajů nebo externím subjektům pokud takové předání není dáno legislativou nebo dohodou se zpracovateli/příjemci OÚ.!

Organizace vyřídí všechny žádosti směřující k plnění práv SÚ podané formou umožňující autentizaci Žadatele. V případě, že ze žádosti není patrné, čeho se žadatel domáhá, bude žádost zamítnuta pro nedůvodnost a žadateli DPO v tomto smyslu odpoví.

Lhůta pro vyřízení žádosti SÚ je 30dnů, v případě, že je třeba delší čas na přípravu, odešle DPO žadateli odpověď ve lhůtě 30dnů od podání v tomto smyslu. Lhůta pro odpověď se může takto prodloužit až o 60 dnů.

12.1 Proces vyřízení žádosti SÚ

1) prvotní reakce na žádost SÚ = kterýkoliv zaměstnanec organizace odkáže Žadatele na pracovníka podatelny, v případě přijetí žádosti v písemné podobě (e-mail s certifikovaným podpisem, pošta, datová schránka) je žádost evidována pracovníkem podatelny v centrální evidenci žádostí SÚ.
2) přijetí = pracovník podatelny žádost o plnění práv subjektem údajů posoudí z hlediska formální správnosti – zda je určena organizaci, zda je úplná, tedy je z ní patrné, čeho se žadatel domáhá. V případě ústního podání provede s Žadatelem zápis žádosti, který SÚ potvrdí. Každou relevantní žádost zapíše pracovník podatelny do centrální evidence žádostí SÚ včetně data podání a kontaktních údajů na žadatele.

3) autentizace SÚ= pracovník podatelny při příjmu žádosti nebo následně prověří, že se jedná o osobu žadatele, resp. osobu oprávněnou za žadatele žádost podat = provede autentizaci osoby žadatele.

Za osobu oprávněnou podat žádost je možné pokládat:

a) Osobu, jež se při osobním kontaktu prokáže občanským průkazem nebo jinou veřejnou listinou prokazující totožnost.
b) Podáním žádosti přes datovou schránku osoby, které se žádost týká
c) Podáním elektronickou poštou v případě podepsání zaručeným elektronickým podpisem (podpis e-mailu, podpis dokumentu žádosti)
d) Podáním podepsané písemné žádosti doručené Organizaci osobně nebo poštou

3) Pracovník podatelny předá veškeré relevantní žádosti SÚ včetně kontaktních údajů SÚ a údajů o datu podání žádosti DPO.
4) O podrobnosti připravené informace v případě nejasností rozhodne vedoucí odboru, popř. tajemník.
5) DPO ve spolupráci s odbornými útvary zajistí plnění práv SÚ a připraví písemnou odpověď žadateli
6) DPO předá vypracovanou odpověď pracovníku podatelny nejpozději 7 dnů před nejzazším termínem odeslání odpovědi žadateli
7) Pracovník podatelny zajistí podpis tajemníkem, popř. starostou města a nejpozději v poslední den lhůty určené na odpověď odešle odpověď žadateli:
    a. Žadatel disponuje datovou schránkou = odpověď bude odeslána datovou schránkou.
    b. Žadatel nedisponuje datovou schránkou
        i. žádost byla podána osobně = pracovník podatelny s žadatelem vyjedná termín osobního převzetí nebo doručení dopisem
        ii. žádost byla doručena poštou = odpověď bude odeslána poštou..

8) Pracovník podatelny zaznamená data a způsob vyřízení žádosti do centrální evidence žádostí SÚ a uloží případné dokumenty do spisu žádosti.

12.2 Typy žádosti SÚ

12.2.1 Žádost o přístup

Subjekt údajů má právo získat od Organizace potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím (obsaženy v Příloze č. 1 Záznamy o činnostech zpracování v řazení dle účelů zpracování):

- účely zpracování;

- kategorie dotčených osobních údajů;

- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

- plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

- existence práva požadovat od Organizace opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a/nebo vznést námitku proti tomuto zpracování;

- právo podat stížnost u dozorového úřadu;

- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách podle článku 46, které se vztahují na předání.

Organizace poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může Organizace účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

DPO zajistí přípravu strukturovanou odpověď na žádost o přístup s obsahem výše uvedených informací, a pokud o to SÚ žádá i kopie dokumentů, které obsahují OÚ žadatele. Při tom nesmí narušit práva a soukromí jiných osob, tedy jiné osobní údaje před odesláním znečitelní. Rozsah poskytnutých kopií určí v každém individuálním případě vedoucí odboru nebo tajemník podle typu žadatele.

12.2.2 Právo na opravu

Subjekt údajů má právo na to, aby Organizace bez zbytečného odkladu opravila nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

Pokud je to možné, DPO zajistí opravu údajů ve všech prostředcích zpracování (osobní spis, datové úložiště, IS).

12.2.3 Právo na výmaz (právo být „zapomenut“)

Subjekt údajů má právo na to, aby Organizace bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a Organizace má povinnost osobní údaje bez zbytečného odkladu vymazat, **pokud je dán jeden z těchto důvodů**:

- osobní údaje **již nejsou potřebné pro účely, pro které byly shromážděny** nebo jinak zpracovány = vyprší stanovená lhůta pro zpracování (viz Spisová a skartační směrnice);

- **subjekt údajů odvolá souhlas**, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;

- subjekt údajů **vznese námitky proti zpracování (v případě použití zákonného důvodu „oprávněný zájem“)** v případě, že neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování v případě přímého marketingu;

- osobní údaje byly zpracovány protiprávně;

- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na Organizace vztahuje;

- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti v souvislosti přímo dítěti a s jeho souhlasem.

Jestliže Organizace osobní údaje zveřejnila a je povinna je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informovala

příjemce a zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

Organizace při obnově ze zálohy provede kontrolu, zda po obnově nejsou OÚ osob, které byly vymazány, opět aktivní. Kontrolu zajistí oddělení IT po provedení obnovy ze zálohy.

12.2.4 Právo vznést námitku

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoliv vznést námitku proti zpracování osobních údajů, které se jej týkají v případě, že je zákonným důvodem oprávněný zájem (GDPR, čl. 6 odst. 1 písmeno f), včetně profilování založeného na těchto ustanoveních. Organizace osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

13. Bezpečnostní incidenty – vyhodnocení rizika, odpovědnosti

13.1 Proces a odpovědnost v oblasti řízení incidentů, kategorie incidentů

1. Všichni zaměstnanci Organizace jsou povinni hlásit potenciální bezpečnostní událost.
2. V případě, že se jedná o událost vzniklou při elektronickém zpracování dat (práce v IS, elektronické verze dokumentů, e-mail, jiná práce na počítači), **hlásí událost přímo vedoucímu IT oddělení, v ostatních případech svému nadřízenému**.
3. Přímý nadřízený nebo vedoucí IT provedou vyhodnocení události a určí, zdali se jedná o bezpečnostní událost nebo incident. O událost se jedná v případě, že došlo k pouze potenciálnímu vzniku škody (např. antivirový systém identifikoval virovou nákazu), incidentem se rozumí událost, při které již vznikla škoda, nebo je třeba okamžité reakce pro zabránění šíření události a vzniku škody – např. ztráta notebooku).
4. Přímý nadřízený nebo vedoucí IT v případě, že vyhodnotí událost jako bezpečnostní incident, provede okamžitě opatření, které zamezí dalším škodám, následně podá informace tajemníkovi.
   Organizace rozlišuje následující kategorie bezpečnostních incidentů:
   a. narušení bezpečnosti informací v IS nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku bezpečnostní události, přičemž v případě porušení dostupnosti a integrity informace se musí jednat o incident, který má dopad na celý IS, modul IS nebo má dopad na více uživatelů. Narušením bezpečnosti rozumíme narušení důvěrnosti, integrity nebo dostupnosti informací, služeb či IS. *Příklad: incidentem je, pokud dojde k zavirování počítače.*
   b. krádeže a hlášení ztrát
   c. narušení schválených pravidel v oblasti fyzické bezpečnosti
   d. narušení schválených pravidel v oblasti personální bezpečnosti
   e. narušení schválených pravidel v oblasti administrativní bezpečnosti
   f. narušení schválených pravidel v oblasti bezpečnosti IT
5. Bezpečnostní událost se v Organizaci neeviduje.
6. Bezpečnostní incident vedoucí IT/přímý nadřízený nahlásí DPO.
7. DPO vždy eviduje Bezpečnostní incident v evidenci bezpečnostních incidentů.
8. DPO následně posoudí (může si vyžádat dodatečné informace od ohlašovatele), zda:
   a. Se ne/jedná o incident s vlivem na osobní údaje/subjekty údajů
   b. V případě, že se jedná o incident s vlivem na osobní údaje/subjekty údajů posoudí riziko pro práva a svobody FO
9. V případě, že se jedná o incident s vlivem na osobní údaje/subjekty údajů, který je třeba ohlásit ÚOOÚ/SÚ informuje o tom ještě před odesláním DPO tajemníka pro potvrzení odeslání informace

Po identifikaci události je nutné rozhodnout o tom, že se jedná o incident s vlivem na osobní údaje/subjekty údajů a o zvýšeném stupni rizika do 72hodin od ohlášení události z důvodu nutnosti ohlášení ÚOOÚ!

O bezpečnostní incident s vlivem na osobní údaje/subjekty údajů se bude jednat v případě, že událost může způsobit fyzickou, hmotnou či nehmotnou újmu, jako např.:

- ztráta kontroly nad OÚ,

- omezení práv SÚ,

- diskriminace,

- krádež nebo zneužití identity,

- finanční ztráta,

- neoprávněné zrušení pseudonymizace,

- poškození pověsti,

- ztráta důvěrnosti OÚ chráněných služebním tajemstvím,

- jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob.

Mezi incidenty s vlivem na osobní údaje lze zařadit např. odeslání přílohy (seznamu OÚ) na jinou adresu nebo krádež notebooku/mobilního zařízení.

Pro určení míry rizika incidentu s vlivem na OÚ/SÚ posuzuje DPO vždy:

a) Rozsah škod = počet dotčených SÚ
b) Množství osobních údajů = rozsah poškození (pouze jméno, příjmení vs. celá platební historie včetně kompletní identifikace SÚ)
c) Citlivost poškozených údajů = kontaktní údaje vs. údaje o zdravotním stavu, platební morálce apod.
d) Způsob poškození = nahodilá a neúmyslná událost vs. cílený a úmyslný útok

V případě, že se bude jednat o incident ohlášený ÚOOÚ, popř. SÚ, sestaví DPO informaci o opatřeních, která pomohla nebo bude řešit daný incident nebo jeho dopady s účelem uvedení této informace do hlášení ÚOOÚ.

Riziko – při posouzení rizika zařadí DPO incident do tří kategorií:

a) Nízké riziko
b) Střední riziko

c) Vysoké riziko

13.2 Ohlášení bezpečnostních incidentů

13.2.1 Riziko střední

DPO jako správce evidence bezpečnostních incidentů v případě, že rozhodne o události, že se jedná o incident s vlivem na osobní údaje/subjekty údajů s mírou rizika **střední**, připraví a odešle ÚOOÚ **hlášení o bezpečnostním incidentu ÚOOÚ**.

Hlášení odešle DPO dle pokynů ÚOOÚ s uvedením informací v minimálním rozsahu:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
b) jméno a kontaktní údaje kontaktního místa, které může poskytnout bližší informace;
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

13.2.2 Riziko vysoké

V případě, že se bude jednat o incident s vlivem na osobní údaje/subjekty údajů s mírou rizika **vysokou**, připraví a **ve spolupráci s odborem kanceláře starosty sestaví seznam dotčených SÚ a následně** odešle **ÚOOÚ a dotčeným subjektům údajů hlášení o bezpečnostním incidentu**, ledaže by byla splněna kterákoli z těchto podmínek:

a) Organizace zavedla náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková,

která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování
b) Organizace přijala **následná opatření**, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví
c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

V oznámení určeném subjektu údajů za použití jasných a jednoduchých jazykových prostředků DPO popíše:

a) povaha porušení zabezpečení osobních údajů
b) jméno a kontaktní údaje kontaktního místa, které může poskytnout bližší informace;
c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Incident je ukončen v závislosti na kategorii rizika pro práva a svobody SÚ:

a) zápisem do evidence bezpečnostních incidentů (nízké riziko)
b) ohlášením incidentu ÚOOÚ a splněním případných pokynů ÚOOÚ (střední riziko)
c) ohlášením incidentu SÚ a splněním případných pokynů ÚOOÚ (vysoké riziko)

13.3 Vyhodnocení incidentu

1. Ex-post vyhodnocení podléhají incidenty se středním a vysokým rizikem pro práva a svobody SÚ
2. Veškeré záznamy o bezpečnostním incidentu jsou po jeho ukončení předány DPO vedoucímu odpovídajícího odboru (popř. IT) k analýze. Cílem analýzy je identifikovat kořenové příčiny a zamezit opakování incidentu.
3. Analýza incidentu, návrh a realizace nápravného opatření je prováděno pracovníky IT nebo pracovníky odpovídajícího odboru. Do 30 dnů od je zpracována a tajemníkovi předána zpráva, která obsahuje:
    a. Časové údaje – kdy došlo k události/incidentu
    b. Jednotlivé činitele – kdo, co
    c. Popis události – jak probíhal incident/událost
    d. Příčiny události – proč k události došlo, např. nový virus AV nezná, uživatel stáhnul atd.
    e. Je ještě uvnitř útočník? Kód, útočník, backdoor?
    f. Uskutečněná opatření před/po zjištění incidentu
    g. Stanovisko ÚOOÚ k incidentu
    h. Návrh na nápravná opatření s termínem uskutečnění nápravných opatření.
4. Tajemník na nejbližší poradě vedení projedná navrhovaná nápravná opatření s cílem jejich přijetí nebo akceptaci stávajícího stavu
5. DPO zajišťuje kontrolu provádění vyhodnocování bezpečnostních incidentů

14. Role Pověřence ochrany osobních údajů

14.1 Jmenování DPO

Pozici DPO je možné:

- Zajistit zaměstnancem Organizace (celý úvazek, část úvazku)
- Zajistit externě (smlouvou o zajištění služby – pro Organizaci nebo sdílením s jinou organizací)
- Sdílet s jinými organizacemi na základě smlouvy nebo jiného právního aktu

Pověřenec (DPO) je jmenován nebo je v případě zajištění smlouvou o zajištění služby Organizaci předány kontaktní údaje na konkrétní osobu, aby byly kontaktní údaje dostupné v souladu s GDPR (SÚ a dozorovému úřadu).

DPO je vždy podřízen tajemníkovi, pokud se jedná o zaměstnance Organizace, je organizačně začleněn do odboru kanceláře starosty. Tajemník zajišťuje DPO materiálním vybavením pro výkon role a vytvořením odpovídajícího fondu pracovní doby pro výkon role.

Ve své činnosti DPO spolupracuje se subjekty osobních údajů (interní i externí), Úřadem na ochranu osobních údajů a všemi organizačními složkami Organizace, představovaných jak jejich vedením, tak jednotlivými zaměstnanci.

DPO nemá přímé podřízené.

14.2 Postavení DPO

DPO je ve výkonu své role zcela nezávislý na vedení Organizace.

DPO není osobně odpovědný za případy nesouladu s GDPR.

DPO nedostává žádné pokyny týkající se výkonu úkolů v oblasti ochrany osobních údajů od vedení Organizace. To znamená, že při plnění úkolů ochrany osobních údajů nesmí DPO dostávat pokyny jak jednat v dané oblasti, například, jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda konzultovat ÚOOÚ.

Pokud Organizace učiní rozhodnutí neslučitelná s GDPR a s radou DPO, musí mít DPO možnost své nesouhlasné stanovisko vysvětlit těm, kteří tato rozhodnutí udělali.

DPO nesmí být ve střetu zájmů a tak nemůže být nucen vykonávat jiné úkoly a povinnosti, které by k němu vedly.

14.3 Informování o DPO

Tajemník zajistí oznámení kontaktních údajů DPO na ÚOOÚ a uvedení kontaktních údajů DPO ve strukturované informaci určené SÚ.

Sdělení kontaktních údajů na DPO vyplývá z povinnosti dle článku 37 odst. 7 GDPR:

d) dozorovému úřadu, tj. Úřadu pro ochranu osobních údajů.
e) Veřejnosti – zveřejnění vhodnou formou (webové stránky, popř. úřední deska) = Kontaktní údaje DPO jsou zveřejněny tak, aby byly dosažitelné subjektům osobních údajů.

Sdělení kontaktních údajů ÚOOÚ lze učinit podle aktuálních pokynů ÚOOÚ (např. využitím elektronických kontaktů (e-mail: posta@uoou.cz, datová schránka: qkbaa2n) s uvedením předmětu zprávy „oznámení pověřence“.

Obsahem sdělení je:

• identifikace správce nebo zpracovatele, který sděluje kontaktní údaje na pověřence

• označení pověřence (jméno, příjmení)

• kontaktní údaje na pověřence (e-mail, popř. telefon)

14.4 Náplň činnost DPO

Role DPO vyvíjí činnosti směřující k dodržování ochrany osobních údajů a zajištění výkonu práv subjektů osobních údajů v souladu s požadavky GDPR a to je:

14.4.1.1 Strategie a plánování (ochrany OÚ, např.):

- rozvoj bezpečnosti informací (v souladu s platnými právními předpisy, bezpečnostními normami s vývojovým trendem informačních technologií, požadavky a potřebami Organizace)
- návrhy bezpečnostních procesů, postupů, strategie, architektury, interních předpisů
- metodické vedení, konzultace a poradenství v oblasti posouzení vlivu, analýz rizik a auditů ochrany OÚ
- kontaktní místo pro zaměstnance Organizace, externí subjekty a dozorové orgány v oblasti ochrany OÚ

14.4.1.2 Pravidelně se opakující kontrolní činnosti (např.):

- kontrola smluvních ujednání se zpracovateli
- poskytování informací a poradenství o povinnostech podle GDPR a dalších platných právních předpisů v oblasti ochrany osobních údajů
- spolupráce s dozorovými orgány v oblasti ochrany OÚ
- monitoring vývoje právní úpravy OÚ, stanovisek dozorových orgánů v oblasti ochrany OÚ, judikatury,
- monitoring vývoje technologií související s ochranou OÚ,
- monitoring souladu navrhovaných řešení v oblasti informačních a komunikačních technologií s pravidly ochrany OÚ
- kontrola shody s legislativou, výklady, nařízeními nadřízených orgánů a judikaturou (ochrana osobních údajů)
- kontrola dodržování bezpečnostních předpisů a opatření
- revize bezpečnostní dokumentace vč. předpisů o ochraně OÚ
- vedení záznamů o činnostech zpracování OÚ
- vyhodnocování bezpečnostních incidentů, případně hlášení určeným orgánům
- kontrola provádění a vyhodnocování bezpečnostního monitoringu
- kontrola ověřování dodržování licenční politiky
- pravidelný reporting o bezpečnostní situaci v oblasti OÚ tajemníkovi Organizace
- pravidelná školení zaměstnanců Organizace v ochraně OÚ

14.5 Práva a povinnosti DPO

14.5.1 Práva DPO

- Účastnit se schůzí vedení Organizace
- Připomínkovat a doplňovat Směrnici ochrany osobních údajů
- Připomínkovat a doplňovat bezpečnostní a pracovní postupy
- Připomínkovat a doplňovat metodiky analýzy rizik a ostatní metodiky v oblasti řízení bezpečnosti a rizik
- Mít přístup na jednání, kde se dělají rozhodnutí s dopadem do ochrany osobních údajů. DPO musí včas obdržet všechny podstatné informace, aby mohl poskytnout odpovídající radu.
- Žádat, aby jeho stanovisku v oblasti ochrany osobních údajů byla vždy přiznána patřičná závažnost. Pro případ nesouhlasu, aby byly zadokumentovány důvody, proč rada DPO nebyla následována.

- Shromažďovat informace za účelem zjišťování zpracovatelských činností ohledně ochrany osobních údajů
- Analyzovat a prověřovat právní soulad zpracovatelských činností ohledně ochrany osobních údajů
- Informovat, radit a vydávat doporučení Organizaci ohledně ochrany osobních údajů
- Navrhovat a po schválení vedením vydávat a/nebo konzultovat bezpečnostní opatření v oblasti ochrany osobních údajů
- Navrhovat a po schválení vedením vydávat a/nebo konzultovat bezpečnostní opatření v oblasti ochrany osobních údajů jako následek bezpečnostního incidentu

14.5.2 Povinnosti DPO

- Pravidelně monitorovat soulad s GDPR v oblasti ochrany údajů a s koncepcemi Organizace v oblasti ochrany osobních údajů a vést odpovídající záznamy
- Upozorňovat na nesoulad s GDPR
- Upozorňovat na rizika ochrany osobních údajů a rizika subjektům osobních údajů
- Poskytovat informace a poradenství zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle GDPR v oblasti ochrany údajů. Poradenství je poskytováno jak ústně, tak telefonicky nebo elektronicky.
- Poskytovat poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů,
- Spolupracovat s ÚOOÚ
- Působit jako kontaktní místo pro ÚOOÚ v záležitostech týkajících se zpracování, včetně předchozí konzultace, a případně vedení konzultací v jakékoli jiné věci.
- Působit jako kontaktní místo pro subjekty údajů
- Sledovat legislativu v oblasti ochrany osobních údajů a upozorňovat vedení Organizace na případné změny
- Vzdělávat se v oblasti ochrany osobních údajů – právo, technická opatření zabezpečení osobních údajů

14.6 Monitorování souladu GDPR

DPO zajišťuje, popř. provádí monitoring souladu s GDPR v oblasti ochrany osobních údajů (více viz kap. 15).

14.7 Analýza rizik

DPO provádí revizi metodiky Analýzy rizik, katalogu klíčových aktiv, hrozeb a zranitelností 1x za 2 roky.

Pro provádění auditu a revize analýzy rizik postupuje DPO podle vlastní metodiky, vedení poskytuje odpovídající písemné výstupy a vyhodnocení revize/auditu, popř. návrhy nápravných opatření.

14.8 Posuzování vlivu na ochranu osobních údajů

DPO spolupracuje s XXX při provádění posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování. Výsledek je předkládán XXX.

DPO spolupracuje při návrhu metodiky pro posouzení vlivu na ochranu osobních údajů.

14.9 Spolupráce s ÚOOÚ

DPO spolupracuje s ÚOOÚ a působí jako kontaktní místo pro ÚOOÚ v záležitostech týkajících se zpracování, včetně předchozí konzultace, a případně vedení konzultací v jakékoli jiné věci.

14.10 Bezpečnostní incidenty

DPO spolupracuje s vedoucími odborů/IT při vyšetřování bezpečnostních incidentů. Zaměstnanci Organizace spolupracují při vyšetřování bezpečnostních incidentů tak, aby bylo možné splnit oznamovací povinnost ÚOOÚ a přijmout opatření zabraňující podobným incidentům v budoucnu.

14.11 Plnění práv Subjektů údajů

DPO slouží jako kontaktní místo a podílí se na procesech výkonu práv subjektu osobních údajů (více viz kap. 12).

15. Provádění kontroly dodržování opatření

Kontrolní činnost a kontrolu provádění bezpečnostních opatření koordinuje DPO v součinnosti s tajemníkem, popř. oddělením IT.

15.1 Monitorování souladu GDPR

DPO zajišťuje a kontroluje provádění monitoringu souladu s GDPR v oblasti ochrany osobních údajů. Monitoring má podobu pravidelného auditu shody.

15.1.1 Audit shody s GDPR

Audit se provádí pravidelně 1x ročně nebo při změně legislativy s dopadem na ochranu osobních údajů.

Oblasti auditu shody:

- Požadavky GDPR
- Bezpečnostní opatření
- Dokumentace

Tajemník ve spolupráci s IT a DPO provádí a koordinuje namátkové kontroly dodržování pravidel ochrany osobních údajů a účinnosti bezpečnostních opatření. Z kontrol je zpracován záznam a v případě negativních výsledků jsou navrhována dodatečná opatření.

Pravidelné kontroly účinnosti opatření:

15.1.2 Kontrola zaměstnanců

- 2 x ročně kontrola organizačního zajištění bezpečnostních opatření – kontrola 3 odborů tak, aby každý odbor byl kontrolován alespoň 1x za 2 roky.

Předmět kontroly – organizační opatření – seznámení všech zaměstnanců odboru s touto směrnicí, seznámení se s Privacy notice pro zaměstnance, kontrola existence ustanovení o mlčenlivosti o OÚ v pracovní smlouvě/DPČ/DPP aktuálně platného znění, revize školení v oblasti ochrany OÚ (obecné principy GDPR, odborná školení).

15.1.3 Kontrola bezpečnostních opatření

u všech zaměstnanců kontrolovaného odboru na místě kontrola fyzického zabezpečení dokumentů v listinné podobě (uložení dokumentů, přítomnost na pracovišti, zamykání, prostor pracovní plochy), zamčení pracovní plochy počítače, kontrola ukládání dokumentů v elektronické podobě, ujištění o tvorbě záloh (spolupráce s IT)

15.1.4 Kontrola nastavení přístupů

Oddělení IT provede 1x ročně kontrolu nastavení přístupů 10 náhodně vybraných uživatelů (plán nastavení přístupů vs. realita), nastavení firewall, nastavení blokování aplikací/webů

15.1.5 IT testování

Nejméně 1x za 2 roky zajistí oddělení IT:

a) test obnovy ze zálohy
b) penetrační test
c) phishing test

15.2 Vyhodnocení kontrol

Vyhodnocení kontrol provede kontrolor písemně se závěrem:

a) bezpečnostní opatření odpovídají aktuálním potřebám
b) bezpečnostní opatření odpovídají aktuálním potřebám, ale dochází k nahodilým a jednotlivým případům porušení – opatřením bude další vzdělávání v oboru a častější kontroly
c) bezpečnostní opatření systematicky neodpovídají aktuálním potřebám – analyzovat situaci, provést revizi opatření, opatření změnit nebo doplnit dodatečná opatření

16. Závěrečné ustanovení

1) Tato směrnice byla schválena RM č. 89 dne 6. 8. 2018, pod bodem RM 89/28.
2) Tímto se ruší Směrnice VP č. 4 o ochraně osobních údajů Městský úřad Horšovský Týn, která byla vydána 22. 7. 2009, a která nabyla účinnosti 1. 8. 2009.
3) Tato směrnice nabývá účinnosti dnem 7. 8. 2018.

.....	.....
Václav Mothejzík v.r.	Ing. Eva Princlová v.r.
starosta	tajemnice MěÚ