Obec Olšany

Olšany 66, 683 01 Rousínov

„Směrnice pro ochranu osobních údajů“

č. 01/2018

Platnost od:	*25.5. 2018*	**Platnost do:**	*31. 12. 2022* *
Účinnost od:	*25.5. 2018*	**Účinnost do:**	*31. 12. 2022* *
	Zpracovatel:	Schvalovatel:	Garant směrnice:
Jméno/subjekt:	Dana Křížová starostka obce Olšany	Dana Křížová starostka obce Olšany	
Podpis:			

ORIGINÁL TOHOTO DOKUMENTU PODLÉHÁ ŘÍZENÍ ZMĚN.

Průběžně dle změn v platné legislativě ČR a organizačních změn vydavatele směrnice, minimálně 1x ročně k 31.12.

Jakékoliv šíření a postupování třetím osobám lze provádět pouze se souhlasem zpracovatele.

* Dne 13. 12. 2022 prodloužena platnost i účinnost do 31. 12. 2030. Dle p. Gubíše nejvýše od vydání legislativní změny.

OBSAH

1 Účel 4
2 Rozsah platnosti 4
3 Základní pojmy 4
4 Související dokumentace 6
4.1 Interní 6
4.2 Externí 6
5 Popis zpracování osobních údajů 6
5.1 Základní povinnosti a práva správce osobních údajů 6
5.1.1 Základní povinnosti správce 6
5.1.2 Základní zásady zpracování osobních údajů 7
5.1.3 Zákonitost zpracování 7
5.1.4 Účel zpracování 8
5.1.5 Souhlas se zpracováním 8
5.1.6 Transparentnost zpracování 8
5.1.7 Účelové omezení 8
5.1.8 Minimalizace údajů 9
5.1.9 Přesnost údajů 9
5.1.10 Omezení uložení údajů 9
6 Ochrana osobních údajů 9
6.1 Úvodní ustanovení 9
6.2 Ochrana osobních údajů v počítačové evidenci 9
6.3 Heslová politika 11
6.4 Zásady pro práci na výpočetní technice 11
6.5 Archivace, skartace, poskytování dat, datová bezpečnost 12
6.6 Vedení evidence SW v počítačích, kontrola nainstalovaného SW v počítačích 13
6.7 Ochrana osobních údajů v papírové evidenci 13
6.8 Technická ochrana osobních údajů 14
7 Práva dotčených osob 15
7.1 Společná pravidla pro výkon práv 15
7.2 Právo na informace 15
7.3 Právo na opravu 16
7.4 Právo na výmaz 16
7.5 Právo na omezení zpracování 17
7.6 Oznamovací povinnost 17
7.7 Právo na přenositelnost údajů 17

7.8 Právo na námitku 17
7.9 Povinnost informovat pověřence 17
8 Odpovědnost správce 18
8.1 Záznamy o činnostech 18
8.2 Ověření zpracovatele a zpracovatelská smlouva 18
8.3 Předávání osobních údajů do zahraničí 18
8.4 Záměrná a standardní ochrana osobních údajů 18
8.5 Posouzení vlivu na ochranu osobních údajů 18
8.6 Kamerový systém 19
9 Řízení bezpečnostních incidentů 19
9.1 Postup 19
10 Povinnost zaměstnanců 19
10.1 Určení rolí pro ochranu osobních údajů 19
11 Doplnění, úprava pracovních náplní zaměstnanců 20
12 Závěrečná ustanovení 20
13 Seznam příloh 20
14 Přehled změn a revizí 20
15 Zkratky 21
Záznam o seznámení zaměstnanců 22

1 Účel

- Nařízení Evropského parlamentu a Rady 2016/679, mění k 25. květnu 2018 právní úpravu ochrany osobních údajů ve všech členských státech EU (dále jen ***„Nařízení“***). Cílem Nařízení je unifikace právní úpravy ochrany osobních údajů ve všech státech EU a zjednodušení postupů správců, kteří zpracovávají údaje ve více státech. Nařízení se vztahuje na všechny, kteří systematicky zpracovávají údaje o osobách fyzických s výjimkou osobního užití a osobních údajů zemřelých osob.
- Účelem a cílem vydání **„Směrnice pro ochranu osobních údajů“,** (dále jen „Směrnice“) je aplikace Nařízení na podmínky Obce Olšany tak, aby bylo dosaženo požadované právní ochrany osobních údajů.

2 Rozsah platnosti

2.1 Směrnice platí pro všechny zaměstnance Obce Olšany. Povinností starosty je prokazatelně seznámit s příkazem své podřízené zaměstnance. Seznámení potvrzují zaměstnanci na formuláři **„Záznam o seznámení zaměstnanců“**, který je nedílnou součástí této Směrnice. Zaměstnanci mají možnost do písemného originálu Směrnice nahlédnout v pracovní době na Obecním úřadě Olšany, a to po předchozí dohodě se starostou.
2.2 Směrnice respektuje rovné příležitosti mužů a žen. Uvedené pojmy, jako jsou např., vedoucí organizačního celku, zaměstnanec, personalista, pověřenec pro ochranu osobních údajů i jiná osoba, označují v textu jak muže, tak i ženy.

3 Základní pojmy

Anonymní údaj – je takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určitému, nebo určitelnému subjektu údajů. V podmínkách obce nebo úřadu jde např. o uveřejňování neadresných údajů o sumě pohledávek po splatnosti, věková struktura zaměstnanců uváděná ve statistických výstupech bez uvedení jednotlivých jmen a podobné souhrnné statistické údaje, které neidentifikují konkrétní osobu.
Balanční test - jde o soubor kritérií, kterým je poměřována váha oprávněného zájmu správce, práva dotčených osob (subjektů údajů) a přiměřenost zásahu do jejich práv. Tento test provádí zodpovědná osoba vždy, kdy zkoumá oprávněnost práv a povinností správce nebo dotčené osoby.
Blokování osobních údajů – vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej zpracovávat.
Informační systém – zahrnuje informační systém úřadu nebo obce, kterým se rozumí funkční celek zabezpečující zpracování agend v SW instalovaném na centrálním serveru, spravovaném úřadem, a informační systém jednotlivých správců, který zahrnuje správu osobních údajů prostřednictvím lokálně nainstalovaných operačních, kancelářských, či jiných SW produktů (MS Windows, MS Excel, MS Word, aj.) přímo na konkrétním PC.
Likvidace osobních údajů – představuje jejich fyzické zničení (např. skartovačem) či vymazání datových nosičů aj. trvalé vyloučení z dalšího zpracování.

Osobní údaj – osobním údajem jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě, kterou nazýváme subjektem údajů. Fyzickou osobu je možné identifikovat přímo nebo nepřímo použitím např. identifikačního čísla nebo jiného identifikátoru. Jakýkoliv údaj, který umožňuje identifikovat konkrétní osobu je osobním údajem.

Pověřenec pro ochranu osobních údajů, (dále jen „pověřenec“) – institut, který zavádí do právního řádu Nařízení Evropského parlamentu a Rady (EU) číslo 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob, v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů v návaznosti na zrušení směrnice číslo 95/46/ES (obecné nařízení o ochraně osobních údajů). Podle článku 37 GDPR je obec povinna jmenovat pověřence.

Shromažďování osobních údajů – systematický postup, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací.

Správce osobních údajů – je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí jejich shromažďováni, zpracování a uchování

Subjekt údajů – je fyzická osoba, ke které se osobní údaj vztahuje. V případě, kdy je vyžadován souhlas subjektu údajů, jde vždy o jednostranný právní úkon tohoto subjektu, jehož obsahem je svolení se zpracováním svých osobních údajů. Subjektem údajů jsou jak zaměstnanci úřadu, tak i třetí osoby (dodavatelé, občané, ...).

Uchování osobních údajů – udržování údajů v takové podobě, stavu, která je umožňuje dále zpracovávat.

Směrnice – je soubor práv a povinností, kterými se při výkonu práce řídí zaměstnanci úřadu-obce. Zpravidla upravuje určitý konkrétní postup či pravidla. Dle míry závaznosti (právní síly) se Směrnice člení na směrnice, řády, příkazy, nařízení, metodické pokyny apod., které mohou mít dlouhodobý či jednorázový charakter, vydávané a schvalované starostou, zastupitelstvem obce. Soubor Směrnice se nazývá soustava, je vedena v elektronické podobě na PC či serveru.

Zpracování osobních údajů - systematický postup, nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič, buď pro okamžité, nebo pozdější zpracování, pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování.

Zpracovatel osobních údajů - je fyzická nebo právnická osoba, která jménem správce zpracovává osobní údaje. Zpracovatel může provádět jen takové operace s osobními údaji, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Zpracovatel plní stanovené povinnosti dle Nařízení a současně pokyny správce ohledně zpracování osobních údajů, od nichž se nemůže na základě vlastního rozhodnutí odchýlit.

Zodpovědná osoba – zaměstnanec v souladu s pracovní činností – pracovní smlouvou či dohodou o pracích konaných mimo pracovní poměr, který nakládá s osobními údaji, za podmínek a v rozsahu stanovených platnou legislativou ČR a EU, upřesněnou nadřízenou osobou a dalšími vnitřními předpisy.

Zvláštní kategorie osobních údajů - jsou de facto tzv. citlivé osobní údaje podle platné legislativy. Zvláštní kategorie osobních údajů 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 fyzické osoby. Nařízení nepovažuje údaj o národnosti za zvláštní kategorii osobního údaje.

4 Související dokumentace

4.1 Interní

„Organizační řád“,
„Pracovní řád“,
„Spisový a skartační řád“,
Vše v platných a aktuálních verzí včetně příp. příloh.

4.2 Externí

ústavní zákon č. 1/1993 Sb., Ústava ČR, v platném znění,
usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Základních práv a svobod, ve znění ústavního zákona č. 162/1998 Sb.,
zákon č. 262/2006 Sb., zákoník práce v platném znění, (dále jen „zákoník práce“),
zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole) v platném znění,
zákon č. 435/2004 Sb., o zaměstnanosti, v platném znění, (dále jen „Zákon o zaměstnanosti“),
zákon č. 255/2012 Sb., o kontrole (kontrolní řád) v platném znění,
zákon č. 586/1992 Sb. o daních z příjmů, v platném znění (dále jen „ZDP“),
zákon č. 187/2006 Sb., o nemocenském pojištění ve znění p. p. (dále jen „ZNP“),
nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů, (dále jen „GDPR“),
Etický kodex úředníků a zaměstnanců veřejné správy, schválený vládou ČR dne 9. května 2012,
norma ČSN 01 6910 (2014) - úprava dokumentů zpracovaných textovými editory.

5 Popis zpracování osobních údajů

5.1 Základní povinnosti a práva správce osobních údajů

5.1.1 Základní povinnosti správce

Správce, prostřednictvím každého zaměstnance, je povinen dodržovat správné a zákonné nastavení a zdokumentování správy osobních údajů subjektů údajů a přijímat všechny relevantní opatření k tomu, aby nedošlo k porušení pravidel stanovených právními předpisy ČR a EU, a to v souladu s touto směrnicí.
Správce odpovídá za zpracování osobních údajů. Nezbytným předpokladem je existence řádného právního důvodu pro zpracování osobních údajů, kterým správce musí disponovat. (viz bod 5.1.3). Zároveň musí osobní údaje dostatečně zabezpečit.

Správce odpovídá:

- za dodržování zásad zpracování,
- za dodržování povinností stanovených Nařízením,
- za zabezpečení údajů.

5.1.2 Základní zásady zpracování osobních údajů

Zodpovědná osoba je povinna respektovat základní zásady pro zpracování osobních údajů jako jsou zákonnost zpracování, transparentnost zpracování, účelové omezení, minimalizace údajů, přesnost údajů, omezení uložení údajů, bezpečnost a integrita dat, doložitelná odpovědnost za soulad s platnými právními předpisy ČR a EU.

5.1.3 Zákonnost zpracování

5.1.3.1 Zodpovědná osoba musí zabezpečit, aby byla dodržena zákonnost zpracování osobních údajů, a musí být schopna doložit existenci právního důvodu ke každému zpracování osobních údajů. Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních důvodů:

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

5.1.3.2 Zákonnost zpracování zvláštní kategorie osobních údajů:

- subjekt údajů udělil výslovný souhlas
- zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů, nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů,
- zpracování je nezbytné z důvodu významného veřejného zájmu,

- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.,
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků,
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.

5.1.4 Účel zpracování
Zodpovědná osoba je povinna jednoznačně a výslovně stanovit účel zpracování. Účel nesmí být stanoven jen obecně.

5.1.5 Souhlas se zpracováním
Zodpovědná osoba získá souhlas se zpracováním osobních údajů od subjektu údajů jen v souladu s platnými právními předpisy ČR a EU. Pokud je zákonné zmocnění ke zpracování osobních údajů uvedeno ve zvláštním právním předpisu, pak správce souhlas nepotřebuje a nebude jej vyžadovat. Zodpovědná osoba je povinna evidovat všechny druhy souhlasů se zpracováním osobních údajů a evidovat je v ***centrální evidenci souhlasů.*** Zodpovědná osoba předá subjektu údajů nezbytné údaje pro transparentnost zpracování (viz níže) a zároveň jej informuje o možnosti a pravidlech odvolání souhlasu.

5.1.6 Transparentnost zpracování
V případě, že zodpovědná osoba shromažďuje osobní údaje přímo od dotčeného subjektu údajů, je povinna mu písemně předat odkaz na internetové stránky správce, kde jsou uvedeny základní informace o zpracování. Správce osobních údajů je povinen zabezpečit, aby pro jednotlivé účely zpracování byl subjekt údajů prostřednictvím internetových stránek informován alespoň o tomto:

- identifikační a kontaktní údaje správce
- kontaktní údaje pověřence
- účel zpracování daných údajů a související právní důvody pro jejich zpracování
- případné vymezení právního zájmu
- případné příjemce nebo kategorie příjemců, kterým mohou být údaje zpřístupněny (státní orgány apod.)

Zodpovědná osoba je povinna posoudit každé jednotlivé zpracování osobních údajů, zda je nezbytné pro spravedlivé a transparentní zpracování.

5.1.7 Účelové omezení
Zodpovědná osoba je povinna dodržovat účelové omezení zpracování osobních údajů, tedy osobní údaje shromažďovat jen pro jasně a předem vyjádřené účely zpracování a nesmí je dále zpracovávat způsobem či pro účely, které jsou s původním účelem neslučitelné. Zodpovědná osoba dále posoudí, zda je další účel či způsob využití osobních údajů přípustný, spravedlivý, legitimní a je očekávatelný ze strany dotčených osob. V případě, že si není jist, obrátí se s písemným dotazem na pověřence.

5.1.8 Minimalizace údajů
Zodpovědná osoba je povinna zabezpečit, aby shromažďovala osobní údaje jen v rozsahu nezbytném pro dosažení sledovaného účelu zpracování.

5.1.9 Přesnost údajů
Zodpovědná osoba je povinna zajistit, aby byly zpracovávány pouze přesné a aktuální osobní údaje. Pokud se věrohodným způsobem dozví, že osobní údaje nejsou přesné nebo již aktuální a správné, je povinna je opravit či vymazat. Zároveň je povinna informovat písemně starostu o této skutečnosti, aby se změna promítla do všech databází a evidencí, ve kterých jsou osobní údaje zpracovávány. O této činnosti bude proveden zápis obdobně jako u **Práva na opravu** (viz bod 7.3).

V případě, že součinnost subjektu údajů nevyplývá přímo ze zákona, je správce osobních údajů povinen tuto povinnost sjednat ve smlouvách.

5.1.10 Omezení uložení údajů
Zodpovědná osoba může osobní údaje uchovávat jen po omezenou a nezbytnou dobu. Doba pro jednotlivé účely je určena podle zákona nebo skartačního řádu. Pokud dobu uchování žádné zvláštní předpisy neupravují, musí je zodpovědná osoba nastavit a odůvodnit sama. Pravidlo nastavování při souběhu více lhůt je stanoveno na nejdelší lhůtu. Pokud si zodpovědná osoba není jista, dotáže se písemně pověřence. Následná likvidace či anonymizace osobních údajů se řídí zvláštním předpisem. Za dodržení těchto postupů jsou zodpovědné nadřízené osoby.

6 Ochrana osobních údajů

6.1 Úvodní ustanovení

Zpracováním dat se rozumí jakákoliv operace nebo soustava operací, které jsou systematicky prováděny s osobními údaji, bez ohledu na to, zda automatizovaně nebo jinými prostředky. Zejména se jedná o shromažďování, ukládání, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování a likvidaci takových údajů.

6.2 Ochrana osobních údajů v počítačové evidenci

Smyslem ochrany dat je učinit taková organizační a technická opatření, která v nejvyšší možné míře omezí možnost nenávratného poškození nebo ztráty dat, minimalizují negativní dopady, způsobené poškozením nebo ztrátou dat, na další činnost organizace. Přijatá technická opatřeni zamezí i přístup k datům nepovolaným osobám.

6.2.1 Za obsahovou správnost, kompletnost a následné uloženi dat v počítačové evidenci v okamžiku pořízení (změny) zodpovídá vždy ten, kdo data pořídil (změnil), bez ohledu na to, odkud byla data získána, či v pracovní náplni zaměstnance je uveden sběr a zpracovaní těchto dat. Zodpovědná osoba, zadávající údaje do počítačové evidence, je povinna, vždy si řádně ověřit věrohodnost a správnost těchto údajů. Zodpovědná osoba, která zjistí

nesrovnalost mezi aktuálně zjištěným údajem a údajem v počítačové evidenci, je povinna tuto skutečnost neprodleně ohlásit příslušnému správci daného údaje a spolupodílet se na zajištění nápravy (viz bod 5.1.9).

6.2.2 Předmětem ochrany jsou veškerá programová vybavení včetně doprovodné dokumentace, všechna provozní data uložená na nosičích informací, v operační paměti počítačů, tiskáren a dalších zařízení výpočetní techniky; záložní a archivní kopie dat uložené na nosičích informací; údaje zobrazené nebo vytištěné na výstupních zařízeních; přístupová hesla, technické informace o informačním systému a návody.

6.2.3 Všichni zaměstnanci, přicházející do styku s výpočetní technikou, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí nenávratnou ztrátu a trvalé poškození provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, poruchou výpočetní techniky, požárem, živelní pohromou, či jinou nepředvídatelnou okolností, atd.

6.2.4 Provozní data, uložena na pevných discích počítačů musí být zálohována v počítačové síti, popřípadě na dalších nosičích. V případě zálohování dat uložených na lokálním disku osobního počítače musí být data uložena v minimálně na dvou od sebe oddělených kopiích (lokální disk, centrální zálohovací systém).

6.2.5 Vytvoření záložní kopie je nutno zajistit (aktualizovat) při jakémkoli pořízení (změně) provozních dat v počítačové evidenci. Pokud nejsou provozní data v průběhu pořízení (aktualizace) ukládána na disk serveru (centrálního počítače), ale pouze lokálně na disk osobního počítače, odpovídá za pořízení záložní kopie provozních dat vždy ten, kdo data pořídil (změnil), bez ohledu na to, odkud byla data získána a zda v pracovní náplni je uveden sběr a zpracování těchto dat. Záložní kopie dat je v těchto případech nutno pořídit (aktualizovat) nejpozději před ukončením pracovní směny v den, kdy byla provozní data pořízena (změněna). Pokud jsou provozní data v průběhu pořízení (aktualizace) ukládána na disk serveru (centrálního počítače), odpovídá za pořízení záložní kopie provozních dat správce. Záložní kopie provozních dat z lokálního disku PC je na záložní disk ukládána ručně. Záložní kopie provozních dat uložených na disku serveru se pořizuje automaticky.

6.2.6 Mezi způsoby ochrany patří zejména - znemožnění jakéhokoli přístupu nepovolaných osob k výpočetní technice, datům a osobním údajům a to jak v pracovní, tak i v mimopracovní době. Nesmí zůstat zapnutá/přístupná výpočetní technika bez dozoru konkrétního zpracovatele (oběd, porady), tj. důsledné odhlašováni se z počítačové sítě při nepřítomnosti na pracovišti. Při odchodu z kanceláře na konci pracovní doby se počítač vypne. Při situování výpočetní techniky na pracovišti musí být dodržena zásada, aby nebylo možno odečítat údaje z monitorů nepovolanými osobami. Dodržet uložení tiskových výstupů mimo dosah nepovolaných osob (i před dalšími zaměstnanci obce). Není dovoleno přesunovat, odpojovat, přenášet, připojovat a ani jinak manipulovat s umístěným zařízením – výpočetní technikou.

6.2.7 Na počítačích mohou pracovat pouze zaměstnanci k tomu pověření, tj. kterým byl počítač přidělen. Zejména počítače, na kterých je zpracováváno účetnictví, mzdová agenda, personalistika musí příslušní zaměstnanci chránit před neoprávněným přístupem, a to nejen přístupovými hesly (odhlášení počítače), ale také zabezpečením místnosti.

6.2.8 Jakoukoli závadu nebo i podezření na nestandardní fungování počítače zaměstnanec, bez zbytečného odkladu, hlásí svému nadřízenému. Do odstranění závady nebo do prověření nahlášeného závadného stavu nesmí zaměstnanci používat technické zařízení v síti (např. v systému elektronického bankovnictví).

6.2.9 Správce sítě je oprávněn v rámci své kompetence monitorovat vytížení sítě a oprávněnost využívání jednotlivými uživateli. Toto ustanovení může být využíváno pro identifikaci přestupků uživatelů v souladu s platnou právní úpravou a dalšími vnitřními předpisy.

6.3 Heslová politika

7.3.1 Uživatelský účet a uživatelské oprávnění umožňuje jednoznačnou identifikaci uživatele při práci s výpočetní technikou a v síti. Součástí uživatelského účtu je i přidělení hesla opravňujícího ke vstupu do sítě. Mimo to vyžadují samostatné heslo i některé sdílené programy a společné datové složky a informační systémy. Prvotní hesla přiděluje a v případě potřeby mění správce sítě.

6.3.2 Uživatel, který oprávněné zná a užívá dané heslo, odpovídá za to, že heslo nesdělí třetí osobě. Je jeho povinností, uchovávat jej na bezpečném místě. Pro tvorbu hesel a používání je nutno dodržovat následující zásady:

a) Heslo musí uživatel uchovávat v tajnosti a chránit jej před zneužitím jinou osobou. Uživatel, který oprávněně zná a užívá dané heslo, odpovídá za to, že jej nesdělí třetí osobě.
b) Je nepřípustné zapisovat si heslo na papír, do datového souboru, apod. Pokud je přesto heslo takto zapsáno, musí být záznam bezpečně uložen.
c) Heslo je tvořeno nejméně osmi znaky, vždy obsahuje kombinaci číslic, malých a velkých písmen a zvláštních znaků. Nesmí být v návaznosti na snadno odhalitelný text obsahující jména, příjmení, známou přezdívku, data narození uživatele používající výpočetní techniku.

6.4 Zásady pro práci na výpočetní technice

6.4.1 Je zakázáno používat nelegální SW; používat SW, jehož použití nebylo schváleno správcem sítě, instalovat bez svolení správce sítě na disky počítačů jakýkoliv SW či data s tímto programovým vybavením související, odstraňovat instalovaný SW, provádět změny v nastavení a umístění SW a souvisejících dat, pořizovat kopie dat pro jinou, než služební potřebu, předávat data jiným subjektům bez předchozího souhlasu starosty, provádět demontáž, úpravy, opravy, změny v nastavení a zapojení prostředků ICT, používat prostředky ICT pro jiné, než schválené účely, např. instalovat a hrát počítačové hry.

6.4.2 Při zahájení práce s ICT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. Ukončování činnosti programů se provádí předepsaným způsobem, včetně ukončení práce v síti. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěřené prostředky, tj. osobní počítače, tiskárny, modemy, atd., vypnuty, s výjimkou těch zařízení, která musí zůstat s ohledem na své určení trvale zapnuta (např. z důvodů zálohování, kamerový systém, ...). Tiskové výstupy, obsahující data podléhající ochraně osobních údajů, musí příslušný zaměstnanec (který tisk provádí) zabezpečit před neoprávněným přístupem neoprávněných osob.

6.4.3 Při ukončení nebo změně pracovně právního vztahu zaměstnance, správce sítě provede úpravu uživatelského účtu zaměstnance, včetně změn přístupových práv.

6.5 Zálohování, skartace, poskytování dat, datová bezpečnost

6.5.1 Pro archivaci dat se na OÚ používá centrální zálohovací systém. Jiné technické nosiče jsou uschovávány pouze na pracovištích OÚ, u zaměstnance v uzamykatelných skříních, v uzamčených pracovních stolech. Není-li uvedeno jinak, ukládají se zálohy dat a vybraných aplikací na samostatném úložišti v jiné místnosti než je centrální úložiště. Pro přenos dat se na OÚ používá síť.

6.5.2 Každý zaměstnanec je povinen provádět zálohování dat uložených na lokálním disku podle rozpisu zálohování. Data jsou zálohována na centrální úložiště. Zálohována jsou výhradně data, nikoli programy nebo operační systém. Zálohy jsou ukládány mimo místnost, kde je počítač umístěn (aby zálohy nemohly být odcizeny nebo poškozeny spolu s počítačem, který je zálohován). Je prováděna vždy plná záloha dát - kompletní kopie všech zálohovaných dat, nikoli jen tzv. přírůstková záloha (data, která se změnila od poslední plné zálohy). Časové provádění záloh se určuje podle druhu prováděných prací, používaných programů, četnosti dat, apod.

6.5.3 Na základě ustanovení § 32 Zákona o účetnictví se doklady osvědčující legální nabytí SW uchovávají po celou dobu užívání licence. Tyto dokumenty tedy není možné skartovat spolu s ostatními doklady v účetnictví. Doklad o nabytí software musí obsahovat jasnou identifikaci dodavatele a odběratele, datum nabytí, specifikaci produktu včetně čísla verze a jazykové mutace, počtu licencí.
OÚ vede přehled o instalaci SW na jednotlivých pracovních stanicích (výpočetní techniky - počítače) a provádí jejich průběžné kontroly. Jakékoli porušení, nedodržení této směrnice hlásí písemně starostovi a pověřenci.

6.5.4 Na počítačích organizace je dle možností používán jeden typ antivirového programu, který je nastaven tak, aby jeho aktualizace byly prováděny automaticky prostřednictvím internetu. Je zakázáno aktivně vytvářet, nebo šířit škodlivé programy a znemožňovat funkci nainstalovaného antivirového programu. OÚ může rozhodnout o využití jiného antivirového programu u počítačů s nižším výkonem, resp. pro potřeby odhalení a následného odstranění specifických typů nežádoucích aplikaci.

6.5.5 Obdrží-li zaměstnanec (elektronickou poštou, na DVD, CD, či jiným způsobem) jakýkoliv soubor zejména z neznámé adresy, nebo o jehož původu lze důvodně pochybovat, je zakázáno soubor otvírat či ukládat na disk. Rovněž je zakázáno spouštět, bez předchozí konzultace se správcem sítě, spustitelné soubory došlé na mediu, elektronickou poštou, či jiným způsobem, zejména soubory s koncovkami *.exe, *.com, *.bat, *.pif, *.vbs, *.vbe, apod.

6.5.6 Zaměstnanec je oprávněn užívat počítač pouze k činnostem souvisejícími s jeho pracovním zařazením, v souladu s licenčními podmínkami a s příslušným návodem k nainstalovanému programu. Je zakázáno stahování (downloading) dat, nebo programů o velkém objemu (např. programové instalace, hudbu, filmy, video, apod.). Zákaz se nevztahuje na automatické aktualizace nabízené systémem a oprávněně užívanými programy. Má-li zaměstnanec podezření na napadení počítače virem, je povinen neprodleně informovat starostu a počítač dále nepoužívat.

6.5.7 OÚ (zaměstnavatel) si vyhrazuje právo, v odůvodněných případech, v souladu s legislativou ČR, přiměřeným způsobem, monitorovat spuštěné programy, přístup na internetové stránky a dobu užívání jednotlivých programů zaměstnanci. OÚ je povinen přímo informovat zaměstnance o rozsahu kontroly a způsobech jejího provádění. Obdobně může OÚ monitorovat počty došlých a odeslaných e-mailů, včetně adres kam je, nebo odkud byl e-mail směřován. Se zjištěnými údaji je nakládáno v souladu s platnou legislativou.

6.5.8 Kromě statistických sledování a hlášení nadřízeným orgánům je zakázáno poskytovat přes internet údaje o OÚ (základní údaje jsou na internetových stránkách obce) a zaměstnancích.

6.6 Vedení evidence SW v počítačích, kontrola nainstalovaného SW v počítačích

Správci sítě vedou podrobnou dokumentaci o legálně nainstalovaném SW v jednotlivých PC zaměstnanců. Provádějí průběžnou kontrolu nainstalovaného SW. V případě zjištění nesrovnalostí neprodleně zajišťují nápravu v souladu se směrnicí zaměstnavatele v návaznosti na platnou legislativu ČR.

6.7 Ochrana osobních údajů v listinné podobě

Každý zaměstnanec (zodpovědná osoba) je ve smyslu Nařízení povinen zachovávat mlčenlivost a chránit před zneužitím data, údaje a osobní údaje zaměstnanců OÚ, klientů OÚ a dalších subjektů obce. Každý zaměstnanec (zodpovědná osoba) je ve smyslu Nařízení povinen shromažďovat pouze nezbytné osobní údaje, bezpečně je ukládat a chránit před neoprávněným přístupem, neposkytovat je subjektům, které na ně nemají zákonný nárok, nepotřebné údaje vyřazovat a dál nezpracovávat. V případě zjištění porušení, výše

uvedených povinností je dotčený zaměstnanec (zodpovědná osoba) povinen konzultovat svá zjištění (písemně oznámit) jmenovanému pověřenci.

6.7.1 Zodpovědná osoba je povinna zabezpečit, aby při jednání s třetí osobou nebyly v dosahu nebo v čitelném dohledu žádné osobní údaje dalších subjektů údajů, které nejsou součástí jednání nebo řízení.
Třetí osoba nesmí zůstat na pracovišti osamocena. V případě, že zodpovědná osoba musí odejít z pracoviště, požádá třetí osobu o opuštění tohoto pracoviště. Při opuštění pracoviště je zodpovědná osoba povinna uzamknout pracoviště.

6.7.2 Podatelna na OÚ
6.7.2.1 Pro příjem pošty jsou stanoveny v jednotlivých dnech tyto časy:
PO = 8 – 16 hod.
ST = 8 – 18 hod.
ÚT, ČT, PÁ = 8 – 11.30 hod.

6.7.3 Pošta bude předávána starostovi, účetní k dalšímu zpracování. Pošta nemůže být veřejně přístupná komukoli.

6.7.4 Všichni zaměstnanci jsou seznámeni se Spisovým a skartačním plánem OÚ v platném znění a jsou povinni jej s ohledem na ochranu osobních údajů dodržovat. Uchovávání tiskopisů je možné jen v souladu s tímto plánem a zodpovědné osoby jsou povinny zabezpečit, aby dokumenty obsahující osobní údaje nebylo možné zcizit.

6.8 Technická ochrana osobních údajů
Každý zaměstnanec OÚ je povinen chránit osobní údaje subjektů údajů před ztrátou, zničením nebo zneužitím.

6.8.1 Budova OÚ a jednotlivé kanceláře jsou zabezpečeny zámky ke dveřím. Hlavní vstup i dveře OÚ jsou zabezpečeny proti volnému průchodu do budovy či místnosti (klika pouze směrem ven). Při denním provozu, kdy jsou dveře hlavního vstupu odemčeny, je možné do budovy vstoupit za použití odemčení, kódového zámku nebo použitím video vrátníku.

6.8.2 Úřad a jím pověřená osoba je povinna vést evidenci svěřených klíčů a přístupových hesel.

6.8.3 Klíče od jednotlivých konkrétních kanceláří, popřípadě jiných prostor, jsou předány jednotlivým zaměstnancům dle dané pracovní pozice při svém nástupu. Za správné zacházení se svěřených klíčem zodpovídá příslušný zaměstnanec.

6.8.4 Všichni zaměstnanci jsou povinni zabezpečit, aby při odchodu z pracoviště byly všechny prostory uzamčeny, okna uzavřena a osobní údaje zabezpečeny.

6.8.5 V případě ztráty klíče je zaměstnanec povinen toto neodkladně nahlásit starostovi a pověřenci. Ti jsou povinni neprodleně rozhodnout o dalším opatření.

7 Práva dotčených osob

7.1 Společná pravidla pro výkon práv

Správce zabezpečí pro výkon práv subjektu údajů snadný přístup k popisům jednotlivých situací pro výkon práv. Na internetových stránkách správce je aktuální popis jednotlivých postupů při uplatňování práv včetně vzorů tiskopisů a kontaktních údajů zodpovědných osob, správce a pověřence.

7.1.1 Správce osobních údajů je prostřednictvím zodpovědné osoby povinen řádně prověřit a jasně identifikovat osobu, která u něj některé z práv uplatňuje, aby nedošlo k záměně osob. V případě elektronického podání je toto možné pouze prostřednictvím datové schránky nebo dokumentem s uznávaným elektronickým podpisem. V případě písemného podání je nutné ověřit totožnost podávající osoby prostřednictvím platných osobních dokladů (OP, cestovní pas apod.). V případě, že bude podání dáno jiným způsobem a nelze jasně identifikovat osobu, odpovědná osoba neprodleně písemně kontaktuje dotčenou osobu a vyzve jí k prokázání totožnosti.

7.1.2 Správce osobních údajů vede evidenci žádostí subjektů údajů o výkon svých práv, kde zapisuje všechny potřebné informace a o každém případě bezodkladně informuje pověřence. Tato databáze musí být vedena pověřencem ve formě tabulky v aplikaci MS Excel.

7.1.3 V případě, že správce prostřednictvím zodpovědných osob má za to, že požadavek na některé z práv subjektu údajů nelze vyřídit z právních nebo jiných důvodů, je povinen bezodkladně písemně seznámit se situací pověřence pro její posouzení a společně do 30 dnů od podání žádosti sdělit důvod odepření žádosti. V případě opakující se žádosti, šikanózní, nedůvodné nebo nepřiměřené žádosti se bezodkladně obrátí na pověřence o konzultaci.

7.2 Právo na informace

7.2.1 Správce pro subjekty údajů eviduje na internetových stránkách obce jednotlivé účely zpracování základních agend obce, kde bude možné se informovat, jaké jsou:

a) účely zpracování
b) kategorie údajů, které správce zpracovává
c) jací jsou příjemci nebo kategorie příjemců osobních údajů
d) plánovaná doba, po kterou budou osobní údaje zpracovávány
e) existence práva subjektu údajů požadovat od správce opravu nebo výmaz osobních údajů, které se jich týkají, omezení jejich zpracování, práv, vznést námitku proti tomuto zpracování a právo podat stížnost u dozorového úřadu
f) veškeré dostupné údaje o zdroji osobních údajů, pokud nejsou získány od subjektu údajů

g) případné skutečnosti, že dochází k automatizovanému rozhodování, které má právní nebo obdobné účinky na subjekt údajů
h) zda jsou nebo nejsou osobní údaje předávány do třetí země mimo Evropskou unii.

7.2.2 Pokud subjekt údajů požádá o zpřístupnění nebo kopie osobních údajů musí správce prostřednictvím zodpovědné osoby připravit informace, které o subjektu údajů zpracovává, ke všem účelům a ke všem právním důvodům, na jejichž základě tak správce činí. Zodpovědná osoba informuje bezodkladně starostu o podání žádosti. Relevantní odpověď předloží (zašle) zodpovědná osoba do 5 dnů od podání žádosti pověřenci k posouzení. Ten se do 20 dnů od podání žádosti písemně (elektronickou či papírovou formou) vyjádří k předloženým dokladům. Zodpovědná osoba dokument případně upraví a zašle jej subjektu údajů do 25 dnů od podání žádosti. Všichni zaměstnanci správce zapojení do tohoto procesu budou především využívat záznamy o činnostech, kde tyto informace jsou shromážděny.

7.3 Právo na opravu

Správce osobních údajů je povinen zajistit, aby byly zpracovávány pouze přesné a aktuální osobní údaje. Pokud se zodpovědná osoba věrohodným způsobem dozví, že osobní údaje nejsou přesné nebo již aktuální a správné, je povinna je opravit či vymazat. Zároveň je povinna informovat písemně starostu o této skutečnosti, aby se změna promítla do všech databází a evidencí, ve kterých jsou osobní údaje zpracovávány. O této činnosti bude proveden zápis.

7.4 Právo na výmaz

7.4.1 Subjekt údajů má právo na výmaz osobních údajů a správce osobních údajů je povinen je vymazat (zapomenout) v případě, že:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány (omezení uložení),
b) subjekt údajů odvolá souhlas se zpracováním a správce údajů nemá žádný právní nebo oprávněný důvod pro jejich zpracování,
c) subjekt údajů vznese námitku proti zpracování prováděnému na základě oprávněného zájmu a správce po balančním testu dospěje k tomu, že práva dotčené osoby v daném případě nad jeho oprávněným zájmem opravdu převažují,
d) pokud jsou zpracovávány osobní údaje pouze pro marketing a subjekt údajů proti tomu vznese námitku,
e) pokud byly správcem osobních údajů zpracovány údaje protiprávně nebo je výmaz správci uložen právem (soud, ÚOOÚ apod.).

7.4.2 Správce osobních údajů není povinen osobní údaje vymazat v případech, kdy po balančním testu zjistí, že oprávněný důvod je silnější než práva subjektu údajů, například:

a) osobní údaje jsou nezbytné ke splnění právní povinnosti správce,
b) pro výkon práva na svobodu projevu a šíření informací,
c) pokud je další zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků a jejich smazání by bylo nepřiměřené a nespravedlivé.

7.4.3 Postup pro výmaz je shodný s článkem 7.3 této směrnice

7.5 Právo na omezení zpracování
V případě, že má subjekt údajů právo na omezení zpracování, správce osobních údajů sice údaje nevymaže, ale jejich aktivní využití dočasně zastaví a zřetelně to označí v jednotlivých databázích. Poté provede balanční test a o této činnosti vyhotoví zápis.

7.5.1 Subjekt údajů má právo na omezení zpracování svých osobních údajů a může ho uplatnit tak, že namítá jejich nepřesnost nebo proto, že uplatnil námitku proti zpracování a tvrdí, že jeho práva převažují oprávněný zájem správce.

7.5.2 Subjekt údajů má právo na omezení zpracování svých osobních údajů a může ho uplatnit tak, že požaduje uchování údajů k ochraně svých práv, byť by byl správce sám povinen tyto údaje vymazat.

7.6 Oznamovací povinnost
Pokud správce, na základě uplatnění práva subjektem údajů, jeho osobní údaje opraví či aktualizuje, vymaže nebo omezí jejich zpracování, je povinen sdělit tuto skutečnost všem případným příjemcům, kterým příslušné údaje zpřístupnil. O této činnosti bude proveden zápis.

7.7 Právo na přenositelnost údajů
Pokud má subjekt údajů právo na přenositelnost údajů, pak je správce povinen na žádost subjektu údajů poskytnout tyto údaje subjektu údajů, nebo třetímu subjektu, kterého subjekt údajů označí, a to ve strukturovaném, běžně používaném a strojově čitelném formátu. Právo na přenositelnost lze uplatnit jen tehdy, pokud správce osobních údajů zpracovává osobní údaje automatizovaně. Správce osobních údajů prostřednictvím zodpovědné osoby provede balanční test a o této činnosti bude proveden zápis.

7.8 Právo na námitku
Pokud zpracovává správce osobní údaje na základě právního důvodu, oprávněného zájmu nebo při výkonu úkolu ve veřejném zájmu, může subjekt údajů proti takovému zpracování uplatnit námitku.

7.8.1 Námitku může subjekt údajů podat na konkrétní situaci, i když nezpochybňuje existenci daného právního titulu, ale dokládá, že v jeho konkrétním případě by zpracování nadále nemělo být prováděno. Správce osobních údajů prostřednictvím zodpovědné osoby provede balanční test a o této činnosti bude proveden zápis.

7.9 Povinnost informovat pověřence
Ve všech případech, kdy se na správce osobních údajů obrací subjekt údajů s uplatněním svých práv, musí být neprodleně písemně informován pověřenec.

8 Odpovědnost správce

Správce je povinen zajistit a doložit, že zpracování osobních údajů je prováděno v souladu s legislativou ČR a EU.

8.1 Záznamy o činnostech zpracování

Správce musí být schopen doložit soulad zpracování osobních údajů s právem. K tomuto účelu jsou vedeny záznamy o činnostech. Zodpovědná osoba je povinna udržovat záznamy o činnostech v aktuálním stavu a ve spolupráci s pověřencem je minimálně jednou ročně kontrolovat a aktualizovat. O této činnosti bude proveden zápis.

8.2 Ověření zpracovatele a zpracovatelská smlouva

Správce je povinen zabezpečit posouzení a průběžné ověřování zpracovatele osobních údajů. Ověření provede správce prostřednictvím zodpovědné osoby tak, aby zpracovatel garantoval dostatečné záruky zavedených vhodných technických a organizačních opatření na zpracování osobních údajů zcela v souladu s platnou legislativou. Pro důvěryhodnost provede správce prostřednictvím zodpovědné osoby tato ověření:

a) identitu zpracovatele, jeho délku existence a popřípadě i majetkovou strukturu
b) další informace z veřejně dostupných rejstříků
c) existenci negativních informací z veřejně dostupných rejstříků (insolvence, databáze dlužníků apod.)
d) existenci zpracovatelova vnitřního systému pro řádné zpracování osobních údajů
e) existenci auditu nebo certifikace pro ochranu osobních údajů zpracovatele.

8.2.1 Pokud je uzavřena smlouva s třetím subjektem smluvně, musí správce osobních údajů uzavřít s takovým zpracovatelem smlouvu nebo dodatek, kde bude specifikována povinnost v souladu s platnou právní úpravou (příloha č. 11).

8.3 Předávání osobních údajů do zahraničí

Pokud jsou předávány informace do zahraničí v rámci Evropské unie (Evropského hospodářského prostoru), lze předávat osobní údaje bez omezení.

8.3.1 Pokud by měly být osobní údaje předávány mimo Evropskou unii (Evropský hospodářský prostor), pak je povinnost správce před tímto požádat pověřence o posouzení vlivu dopadu na práva subjektu údajů při takovémto postupu. O této činnosti bude proveden zápis.

8.4 Záměrná a standardní ochrana osobních údajů

Správce osobních údajů prostřednictvím zodpovědných osob je povinen při každém zpracování osobních údajů zabezpečit, aby byly zpracovávány osobní údaje pouze v rozsahu nezbytně nutném k dosažení daného účelu.

8.5 Posouzení vlivu na ochranu osobních údajů

Správce je povinen prostřednictvím zodpovědných osob průběžně posuzovat rizikovost zamýšleného zpracování jednotlivých osobních údajů podle účelu, povahy, kontextu a

rozsahu. V případě, kdy vyhodnotí, že nové zpracování může představovat vysoké riziko, o tomto písemně informuje neprodleně pověřence. O této činnosti bude proveden zápis.

8.6 Kamerový systém

Správce provozující kamerový systém odpovídá za zpracování osobních údajů, které jeho prostřednictvím provádí. Zaměstnavatel zavádějící kamerový systém je povinen postupovat v souladu s ustanovením § 316 odst. 2 zákoníku práce.

9 Řízení bezpečnostních incidentů

Bezpečnostním incidentem je jakékoli porušení bezpečnostních pravidel vedoucích k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů, ať už v listinné nebo datové podobě, v telefonu, tabletu, počítači či na jiném obdobném zařízení sloužícímu ke služebním účelům.

9.1 Postup

10.1.1 Správce osobních údajů prostřednictvím zodpovědných osob je povinen každý jednotlivý bezpečnostní incident bezprostředně písemně detailně popsat a oznámit pověřenci.

9.1.2 Správce osobních údajů je povinen prostřednictvím zodpovědných osob vést evidenci všech incidentů, včetně těch, které nikomu neoznamuje. Součástí záznamů jsou i nápravná opatření k zamezení opakování incidentu.

9.1.3 Pokud správce osobních údajů prostřednictvím zodpovědných osob zjistí zanedbatelné či velmi malé riziko, je povinen jej zaevidovat a posoudit, zda je nutno přijmout nápravná opatření (individuální či systémová).

9.1.4 Pokud správce osobních údajů prostřednictvím zodpovědných osob zjistí nízké či střední riziko, je povinen jej zaevidovat, řešit a oznámit ÚOOÚ.

9.1.5 Pokud správce osobních údajů prostřednictvím zodpovědných osob zjistí vysoké riziko, je povinen jej zaevidovat, řešit, oznámit ÚOOÚ a dotčeným osobám (subjektům údajů).

10 Povinnost zaměstnanců

Každý zaměstnanec je ve smyslu evropského nařízení ke GDPR povinen zachovávat mlčenlivost a chránit před zneužitím data, údaje a osobní údaje zaměstnanců obce, klientů obce a dalších subjektů.

10.1 Správce je povinen zajistit osvětu a kvalifikované školení zaměstnanců minimálně jednou ročně.

11 Doplnění, úprava pracovních náplní zaměstnanců

Pracovní náplně se doplňují následujícím textem:
„Zaměstnanec ohlašuje, bez zbytečného odkladu, zaměstnavateli veškeré negativní skutečnosti, navrhuje zlepšení a nápravu procesů, které jsou nezbytné pro ochranou osobních údajů. Zachovává mlčenlivost, chrání před zneužitím:

a) osobní data, údaje a osobní údaje klientů, své i zaměstnanců OÚ,
b) citlivé osobní údaje, informace o zdravotním stavu klientů, zaměstnanců
c) a další informace, se kterými přichází do styku v souvislosti s výkonem práce v rámci pracovněprávního vztahu k OÚ.

12 Závěrečná ustanovení

12.1 Aktuální verze této směrnice je dostupná na webu úřadu.

12.2 Návrhy na změnu této směrnice mohou být podány u zpracovatele směrnice. Změny jsou prováděny formou číslovaných písemných dodatků.

12.3 Tato vnitřní směrnice musí být operativně doplňována podle získaných zkušeností, změn v legislativě nebo organizačních změn popřípadě na základě požadavků kontrolních orgánů.

13 Seznam příloh

Příloha č. 1 - Záznam o instruktáži týkající se zpracování osobních údajů zaměstnance

Příloha č. 2 - Souhlas se zpracováním osobních údajů, vzor

Příloha č. 3 - Souhlas se zpracováním osobních údajů, pro stávajícího zaměstnance

Příloha č. 4 - Souhlas se zpracováním osobních údajů, pro uchazeče o zaměstnání

Příloha č. 5 - Souhlas se zpracováním a zveřejněním osobních údajů, pro zastupitele obce

Příloha č. 6 - Souhlas se zpracováním a zveřejněním osobních údajů, z důvodu zveřejnění informací na webu obce – údaje o firmě

Příloha č. 7 - Souhlas se zpracováním a zveřejněním osobních údajů, z důvodu zveřejnění

Příloha č. 8 - Prohlášení zpracovatele o ochraně osobních údajů

Příloha č. 9 - Vzorová smlouva mezi správcem a zpracovatelem v oblasti zpracování osobních údajů zpracovatelem pro správce

14 Přehled změn a revizí

Změna číslo:	Strana změny:	Předmět změny:	Provedl:	
			Datum:	Jméno-zařazení-podpis:
Verze 1		**Nově vydaná směrnice**		

15 Zkratky

EZS - Elektronický zabezpečovací systém
GDPR - Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
ICT - prostředky informační a komunikační technologie
ISO - Mezinárodní organizace pro normalizaci (International Organization for Standardization)
OÚ - Obecní úřad
PC - Personal Computer (osobní počítač)
Směrnice - vnitřní organizační předpis
SW - (software), programové vybavení PC, počítačový program
ÚOOÚ - Úřad pro ochranu osobních údajů
ve znění p. p. - ve znění pozdějších předpisů

Záznam o seznámení zaměstnanců

Obce Olšany, zařazených do Obecního úřadu Olšany,

se směrnicí č. 01/2018

„Směrnice pro ochranu osobních údajů“,

která byla vydána dne 25. 05.2018.

Směrnice je přístupná v elektronické podobě na webu obce a v písemné, originální podobě u starosty obce.

P.č.	Jméno a příjmení zaměstnance:	Seznámen dne:	Podpis:	Poznámka:
1	Štefanie Hrubá	25.5.2018		
2	Alena Mikysková	25.5.2018		
3	Eva Kuncová	25.5.2018		
4	Milan Sotolář	25.5.2018		
5	Marcela Schneiderová	24.5.2018		
6	Ing. Eva Modlitbová	25.5.2018		
7	Tomáš Kubl—	2.12.2019		