OBEC KLADNO

Kladno 84, 539 01 Hlinsko v Čechách

SMĚRNICE č. 1/2018

schválená na zasedání Obecního zastupitelstva dne 22. 5. 2018, pod číslem usnesení 4/2018
Tato Směrnice stanovuje vnitřní pravidla pro zajištění ochrany osobních údajů a plnění povinností podle Obecního nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.

PŘEDMĚT SMĚRNICE A ZÁKLADNÍ USTANOVENÍ

- Touto Směrnicí Obec Kladno /dále jen „ obec“/ stanovuje vnitřní pravidla pro zajištění ochrany osobních údajů a plnění povinností podle Obecného nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů jakožto přímo účinného předpisu EU /dále též „Obecné nařízení“/ a podle zákona o zpracování osobních údajů /dále též „zákon“, zejména při zpracování osobních údajů vykonávaných obcí, zejména jejím obecním úřadem /“dále jen OÚ“/.
- Ustanovení této Směrnice jsou závazná pro všechny osoby v rámci obce, zejména pro zaměstnance obce /“dále jen zaměstnanci“/. Obdobně jako pro zaměstnance je tato směrnice závazná i pro členy orgánů obce, jako jsou členové zastupitelstva, komisí a výborů /dále jen „členové orgánů“/, pokud se v souvislosti s výkonem své funkce seznamují, případně zpracovávají osobní údaje.
- Jakékoliv smlouvy, podle kterých osobní údaje zpracovávají anebo se s nimi seznamují při plnění smlouvy uzavřené s obcí další osoby /dále jen „zpracovatelé a další smluvní osoby“/, musejí být písemné /včetně elektronické formy/ a obsahují závazek k dodržování této směrnice, konkretizaci povinností podle směrnice a potvrzení, že smluvní strana se se směrnicí seznámila.
- Pokud pro obec zajišťuje zpracování osobních údajů v rámci plnění smluvních povinností jiný subjekt /zpracovatel/, pak musí být v rámci smluvních vztahů zaručeno plnění povinností podle Obecného nařízení a podle této směrnice a musí být upravena odpovědnost za tyto činnosti vůči správci a vůči kontrolním orgánům. Náležitosti smlouvy o zpracování osobních údajů upravuje Obecné nařízení.

ZÁKLADNÍ POJMY

Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon. V souladu s tím je

- **Osobním údajem** jakákoli informace týkající se identifikované nebo identifikovatelné fyzické osoby /dále jen „subjekt údajů“/, identifikovatelnou fyzickou osobou je osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, IČO, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
- **citlivým osobním údajem** je osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení či členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Osobní údaje týkající se rozsudků v trestních věcech a trestných činů se pro účel této směrnice hodnotí obdobně jako citlivé osobní údaje

- **zpracováním osobních údajů** 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, přizpůsobení nebo
- pozměnění , vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení, za zpracování osobních údajů se nepovažuje pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu /schůze, kulturní, společenské, sportovní akce/, aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje /1/
- **subjektem údajů** fyzická osoba, k níž se osobní údaje vztahují
- **souhlasem subjektu údajů** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

OSOBNÍ ÚDAJE A JEJICH ZPRACOVÁNÍ

1. Způsob zpracování osobních údajů a pověřené osoby

1.1. Osobní údaje lze zpracovávat pouze za podmínek stanovených Obecným nařízením, případně zvláštními zákony, přičemž je nezbytné dodržovat ustanovení této směrnice. Zpracovávat lze pouze osobní údaje získané zákonným způsobem

1.2. Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou

1.2.1. Zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů

1.2.2. Člen orgánu, pokud je to nezbytné pro výkon jeho funkce

1.2.3. Osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.

2. Účel zpracování , zákonnost a nově zaváděné účely zpracování /2/

2.1. Veškerá zpracování osobních údajů probíhají v rámci jednotlivých agend, tzv. „účelech zpracování „. Ten, kdo rozhoduje o činnosti zpracování /dále jen „odpovědný zaměstnanec“/, pro každé zpracování /agendu, evidenci/ stanoví účel zpracování, tedy jeho výstižný a konkrétně vymezující popis v rozsahu několika slov. O účelu drobných zpracování /tj. zpracování s nízkým rizikem/**3/** rozhoduje osoba, do jejíž kompetence spadá úkol, který zpracování osobních údajů vyžaduje. V případě, kdy lze předpokládat, že účel zpracování zasahuje subjekty osobních údajů ve velkém rozsahu, povinna předložit stanovení účelu k rozhodnutí svému starostovi, případně svému nadřízenému.

2.2. Právní titul či tituly /4/ každého účelu zpracování určí odpovědný zaměstnanec. V případě, kdy agenda obsahuje také citlivé osobní údaje, určí zároveň právní titul pro citlivé údaje. K obojímu určí také právní základ, je-li potřebný

2.3. Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu a navrhne nezbytný rozsah údajů pro dané zpracování, dobu a způsob uchování a způsob informování subjektu údajů

2.4. Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec vyžádá posouzení pověřencem.

1/ Stanovisko č. 12/2012-k použití fotografie,obrazového a zvukového záznamu fyz.osoby

2/ čl. 5 odst. 1 písm. a/ a b/ Obecného nařízení

3/ čl. 33 odst. 1 ON, kdy není pravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob

4/ Právním titulem je některé ustanovení čl. 6 odst. 1 písm. a/ až f/, čl. 9/2 písm. a/ až j/ čl. 10 ON

2.5. O každém nově zamýšleném účelu zpracování je ten, kdo navrhuje jeho účel, povinen informovat pověřence, a to před jakýmkoli krokem, který vyvolává závazek nebo náklady obce. Zahájit novou činnost zpracování lze jen na základě doložitelného posouzení pověřencem.

2.6. Pověřené osoby jsou povinny zpracovávat osobní údaje pouze ke stanovenému účelu, v rozsahu pracovní náplně a úkolů, které jim byly stanoveny jejich nadřízenými anebo vyplývajícím z jejich funkce , a na místech k tomu určených. Jsou povinny dodržovat základní zásady při zpracování osobních údajů.

2.7. Ustanovení tohoto článku se přiměřeně vztahuje i na člena orgánu při výkonu jeho funkce, který spolupracuje s odpovědným zaměstnancem a pověřencem.

3. Zásady zpracování osobních údajů

3.1. Základní zásady při zpracování osobních údajů jsou:

3.1.1. zpracovávat osobní údaje korektním a transparentním způsobem

3.1.2. před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování

3.1.3. zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu

3.1.4. zpracovávat osobní údaje přesně a podle potřeby je aktualizovat

3.1.5. zajišťovat náležité zabezpečení osobních údajů.

4. Záznamy o zpracování a kontrolní seznam

4.1. Každý odpovědný zaměstnanec vede ve formuláři, jímž byla provedena implementace Obecného nařízení /dále jen „Kontrolní seznam“/

4.1.1. Záznamy o příslušných účelech zpracování /dále jen „záznam o zpracování“/5/

4.1.2. Záznamy o provedených opatřeních k dosažení souladu s Obecným nařízením, jako je šifrování, likvidace či výmaz dat, lhůty pro likvidaci, forma a lhůty zálohování

4.1.3. Záznamy o bezpečnostních incidentech jako je únik, ztráta, neoprávněný přenos či zveřejnění

4.1.4. Další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektu údajů

4.2. Ke kontrolnímu seznamu mají přístup odpovědní zaměstnanci a pověřenec. O změnách v kontrolním seznamu musí odpovědní zaměstnanci vždy informovat pověřence, např. sdílením aktualizované verze

4.3. Starosta nebo jím určená osoba zajistí pravidelné zálohování kontrolního seznamu a případných souvisejících dokladů.

5. Doklady o souladu s Obecným nařízením

5.1. Každá pověřená osoba, pokud to plyne z náplně její práce, dbá na uchování dokladů opravňujících určité zpracování osobních údajů, jako jsou

5.1.1. Smlouvy, pro jejichž plnění se zpracovávají osobní údaje

5.1.2. Doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu

5.1.3. Doklady o vyřízení žádosti subjektu údajů

5.1.4. Souhlasy se zpracováním osobních údajů

5.1.5. Balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby

5.1.6. Evidence klíčů, je-li potřebná

5.1.7. Evidence přístupů do počítačů a přístupových práv v informačním systému, je-li potřebná

5/ čl. 30 Obecného nařízení

5.1.8. Údaje o zpřístupnění kamerového systému či dalších specifických záznamů osobních údajů

5.1.9. Další obdobné doklady

5.2. Tyto doklady vede odpovědný zaměstnanec v kontrolním seznamu, pokud to jejich povaha umožňuje, jinak se v kontrolním seznamu pouze uvede, kde jsou uloženy.

6. Práva subjektů údajů

6.1. Informování subjektů údajů/ 6/

6.1.1. Odpovědný zaměstnanec zajistí informování subjektů údajů, jejichž údaje obec zpracovává, zejména na webu obce, případně při uzavření smlouvy nebo získání souhlasu se zpracováním. Zajistí též stručný, transparentní, srozumitelný a snadno přístupný způsob těchto sdělení /7/

6.1.2. Odpovědný zaměstnanec zajistí také doložitelnost uvedeného informování. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci.

6.2. Přístup k osobním údajům /8/

6.2.1. Požadavky subjektů údajů vyřizuje odpovědný zaměstnanec. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci. Pro vyřízení se přiměřeně postupuje podle obecného předpisu pro přístup k informacím /zákon č. 106/1999 Sb./, neuplatní se správní řád.

6.2.2. Požádá-li subjekt údajů o sdělení svých osobních údajů, ověří se totožnost žadatele a potvrdí na žádosti, případně se ověření totožnosti k žádosti přiloží, např. číslo průkazu , podle kterého byla ověřena, ověření uznávaného elektronického podpisu, datové schránky /“dále jen ověření totožnosti“/.

6.2.3. Běžné provozní dotazy týkající se osobních údajů /zejm. informace o zpracování osobních údajů/, vyřídí zaměstnanec podle okolností co nejdříve.

6.2.4. K vyřízení ostatních žádostí o přístup k osobním údajům /zejm. export údajů/ je příslušný odpovědný zaměstnanec. Žádost se vyřídí do 30 dnů.

6.2.5. V případě potřeby a s ohledem na složitost a počet žádostí může odpovědný zaměstnanec prodloužit lhůtu vyřízení žádosti o další dva měsíce, přičemž o tom informuje subjekt údajů do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

6.2.6. Jestliže subjekt údajů podává žádost v elektronické formě a je-li to možné, poskytnou se informace v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob.

6.3. Právo na výmaz, opravu a doplnění

6.3.1. Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů.

6.3.2. Subjekt údajů má právo žádat o výmaz, opravu a doplnění osobních údajů, které se ho týkají /9/ . Případy, kdy je požadavek na výmaz oprávněný, stanoví čl. 17,odst. 1 a 3 Obecného nařízení. Žádost vyřídí odpovědný zaměstnanec po ověření totožnosti a po prověření oprávněnosti požadavku ihned, jakmile je to možné, nejdéle do 30 dnů, čl. 6.2.5. Směrnice se použije obdobně. Pokud má ověření oprávněnosti požadavku trvat delší dobu, zejména by se osobní údaje dotčené žádosti měly zpracovávat ke stanovenému účelu zpracování /např . zaslat pravidelné vyúčtování s chybným údajem

---

6/ čl. 13 a 14 Obecného nařízení

7/ čl. 12 Obecného nařízení

8/ čl. 15 Obecného nařízení

9/ čl. 16, 17 Obecného nařízení

zajistí jejich vyřazení ze zpracování /10/ a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.

6.3.3. Oznámí-li subjekt údajů /např. telefonicky nebo emailem/, že osobní údaje , které se ho týkají , se změnily, a nelze dodatečně ověřit jejich totožnost s ohledem na závažnost požadované změny /např. na základě osobní znalosti hlasu, znalosti e-mailové adresy/, vyzve ho odpovědný zaměstnanec k postupu, umožňujícímu totožnost ověřit.

6.3.4. Zjistí-li pověřená osoba při své činnosti, že při zpracování osobních údajů došlo ke zjevné chybě v psaní /např. překlepu/, informuje odpovědného zaměstnance a údaj opraví.

7. Pověřenec na ochranu osobních údajů

7.1. Pro obec vykonává úkoly pověřence pro ochranu osobních údajů Bc. Kristýna Vodrážková, e-mailová adresa: kristyna.vodrazkova@sms-sluzby.cz, telefon 608 980 091.

7.2. Starosta zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.

7.3. Všechny pověřené osoby jsou povinny /11/

7.3.1. Konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením

7.3.2. Poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování

7.3.3. Zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem

7.3.4. Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě.

8. Bezpečnost informací

8.1. Obecné postupy při zabezpečení osobních údajů

8.1.1. Přiměřeně zabezpečeny musí být zpracovávané osobní údaje i ty, které nejsou systematicky zpracovávané, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech

8.1.2. Úroveň zabezpečení lze přiměřeně snížit u osobních údajů, u nichž je riziko pro subjekty údajů nepatrné nebo jsou běžně dostupné veřejnosti, zejména o zaměstnancích a členech orgánů, dalších osobách

8.1.2.1. Na základě zákona o svobodném přístupu k informacím

8.1.2.2. Jsou veřejně dostupné /například ve veřejně přístupných registrech/

8.1.2.3. Nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací

8.1.3. V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.

8.1.4. Osobní údaje musí být zabezpečeny před neoprávněným nebo nahodilým přístupem k nim, proti jejich změně, zničení či ztrátě /zejména dostatečné zálohování/, neoprávněným a nezabezpečeným přenosům, proti jejich jinému neoprávněnému zpracování, jakož i proti jinému zneužití osobních údajů. Zabezpečení spočívá při nepřítomnosti pověřených osob zejména v uchování záznamových médií /písemných nebo elektronických/, obsahujících osobní údaje, v uzamčených skříních, v uzamykání kanceláří a jiných míst a dále v dodržování pravidel informační bezpečnosti.

11/ „omezení zpracování“

12/ čl. 38 Obecného nařízení

8.1.5 Dále jsou pověřené osoby povinny vyvarovat se jakéhokoliv jednání, které by mohlo být chápáno jako neoprávněné zveřejňování osobních údajů, nebo vést k neoprávněnému přístupu třetích osob k osobním údajům. Zejména, ale nikoliv pouze:

8.1.5.1. sdělovat jakékoli osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem

8.1.5.2. hlasitě sdělovat osobní údaje ve veřejně přístupných prostorách

8.1.5.3. umožnit nepovolaným osobám nahlížet do listin, které nesou osobní údaje, nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny

8.1.5.4. sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo nařízením.

8.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje

8.2.1. Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být mimo dobu, kdy jsou pod dohledem zaměstnanců, zabezpečeny v uzamčených skříních, popř. na jiných místech zajišťujících jejich ochranu. To platí i pro kopie písemností a digitální zálohy, obsahující osobní údaje.

8.2.2. Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

8.3 Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích

8.3.1. Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů.

8.3.2. Pevné počítače s přístupem k osobním údajům musí mít alespoň zabezpečený přístup do počítače /přihlášení pod heslem/ a nastaveno uzamčení obrazovky po době nečinnosti nejvýše 5 minut.

8.3.3. Významné evidence osobních údajů /například mzdová, personální agenda, rozsáhlá evidence obyvatel s dalšími , zejména kontaktními údaji typu evidence svozu komunálního odpadu/, musí být zabezpečeny také zvláštním přístupem do programového vybavení anebo být jako soubor šifrované.

8.3.4. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložiště pomocí šifrovacího programu

8.3.4.1. zajištěna šifrováním disku či jiného uložiště pomocí šifrovacího programu

8.3.4.2. zajištěna zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně

8.3.4.3. být jako soubor šifrované

8.3.4.4. je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizována, nebo

8.3.4.5. pokud přenosné médium sloužilo jen k přenosu, bezodkladně po přenosu bezpečně vymazána /12/

8.3.5. Pověřené osoby pravidelně posuzují úroveň zabezpečení informačních systémů včetně přenosu dat s ohledem na rizika ro subjekty osobních údajů a v případě potřeby přijímají vhodná technická a organizační opatření, aby rizika zmírnily /13/

8.3.6. Pověřené osoby zejména dbají na dostatečnou kvalitu hesel /nejméně 8 znaků, obsahuje minimálně 3 ze 4 položek: Velká písmena, malá písmena, čísla, symboly, jako pomlčka či lomítko/ pravidelné obměny hesel a je-li to možné vzhledem k nutné zastupitelnosti, důvěrnosti pouze pro jednoho uživatele. V případě potřeby ukládají hesla zabezpečeně a zcela odděleně od počítačů a médií, na nichž jsou použita.

13/ k vymazání nepostačí pouhé vymazání z adresáře

14/ čl. 32 nařízení

8.3.7. Přenos souborů s osobními údaji nezabezpečenou sítí Internet /např. protokol http/ a jejich uložení na nezabezpečených uložištích /běžné e-mailové schránky, přechodná uložiště jako Úschovna.cz/ je přípustný jen se zašifrováním souboru a předáním hesla příjemci jinou cestou , například SMS zprávou na ověřené číslo telefonu či pomocí jiné zabezpečené aplikace

8.3.8. Umožňuje-li to programové vybavení, pověřené osoby vždy využijí možnosti záznamu přístupů a činnosti /auditního záznamu, logu/ na počítačích nebo v informačním systému. Záznamy pravidelně kontrolují. Tímto úkolem může být pověřen určený zaměstnanec

8.3.9. Za plnění povinností stanovených v tomto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

9. Porušení zabezpečení a míra jeho rizika

9.1. Zjistí-li kdokoliv, že došlo k fyzickému nebo elektronickému porušení zabezpečení osobních údajů, např. úniku, ztrátě, zničení, neoprávněnému zveřejnění osobních údajů /dále jen „incident“/, neprodleně o tom informuje pověřence, odpovědného zaměstnance, starostu nebo místostarostu.

9.2. Odpovědný zaměstnanec vyhodnotí riziko pro práva a svobody fyzických osob a konzultuje s pověřencem. Pokud ve shodě s pověřencem posoudí jako nepravděpodobné, že by incident měl za následek riziko pro práva a svobody fyzických osob /dále jen „nízké riziko“/, provede o incidentu záznam k příslušnému účelu zpracování v kontrolním seznamu. Pokud vyhodnotí, že nejde jen o nízké riziko, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl některých odpovědný zaměstnanec /14/
Pokud jde o riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstna-nec vhodným způsobem navíc informuje subjekty údajů. /15/ Pokud v konzultaci s pověřencem však vyhodnotí, že již existuje či lze přijmout opatření, díky němuž se vysoké riziko pro subjekty údajů neprojeví anebo by informování vyžadovalo nepřiměřené úsilí, pouze zveřejní informaci o incidentu na webu obce na výrazném místě.

10. ZÁVĚREČNÁ USTANOVENÍ

10.1. Kontrola dodržování směrnice

10.1.1. Starosta případně místostarosta zajistí kontrolu plnění povinností vyplývajících z usta-novení Směrnice pro nakládání s osobními údaji

10.1.2. Starosta případně místostarosta zajistí, aby s dokumentem Směrnice pro nakládání s osobními údaji byli seznámeny všechny pověřené osoby , další zaměstnanci, dodavatelé, kteří mohou přijít jakýmkoli způsobem do styku s osobními kontakty.

10.2. Revize směrnice

10.2.1. Revize směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky

10.2.2. Za zpracování, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá starosta nebo jím pověřená osoba

10.2.3. Revize směrnice se provádí na základě konzultace s pověřencem pro ochranu osobních údajů

14/ čl. 33 Nařízení

15/ čl. 34 Nařízení

10.3. Účinnost směrnice

Směrnice pro nakládání s osobními údaji nabývá účinnosti a platnosti dnem vydání.

……..	……	……
JUDr. Eliška Kernerová	Mgr. Eva Pejchová	Jaroslav Drahoš
Starostka	místostarostka	místostarosta

V Kladně dne 22. května 2018