Směrnice č. ~~02~~ 01/2018

GDPR o ochraně osobních údajů

(dále též pouze „Směrnice")

Obec	Statenice
IČO	00241679
Zpracoval	Bc. Nela Kubásková, pověřenec pro ochranu osobních údajů
Účinnost od	19.12.2018
Platnost	Dnem podpisu starostou obce

1. Účel a předmět Směrnice, základní ustanovení

- Účelem této Směrnice je stanovit postup ochrany osobních údajů ve smyslu zákona č. 101/2000 Sb. o ochraně osobních údajů, v platném znění, resp. požadavků NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 - obecné nařízení o ochraně osobních údajů (dále též pouze „GDPR"), v organizaci správce. Pro účely této Směrnice se správcem rozumí Obecní úřad Statenice. Směrnice dále upravuje povinnosti zaměstnanců organizace správce při ochraně údajů zpracovávaných organizací správce.
- Ustanovení této Směrnice jsou závazná pro všechny osoby v rámci organizace správce, zejména pro zaměstnance správce (dále též pouze „zaměstnanci"). Obdobně jako pro zaměstnance je tato Směrnice závazná i pro členy orgánů města, jako jsou členové zastupitelstva, komisí a výborů (dále též pouze „členové orgánů"), pokud se v souvislosti s výkonem své funkce seznamují, případně zpracovávají osobní údaje.
- Pokud pro správce zajišťuje zpracování osobních údajů v rámci plnění smluvních povinností jiný subjekt (zpracovatel), pak musí být v rámci smluvních vztahů zaručeno plnění povinností podle GDPR 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 GDPR.

2. Oblast platnosti

Ustanovení této Směrnice jsou platná v celé organizaci správce.

3. Definice pojmů podle GDPR a zkratky

3.1. Definice pojmů

- **Správce:** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

- **Subjekt údajů:** fyzická osoba, k níž se osobní údaje vztahují.

- **Osobní údaj:** jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (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.

- **Zpracování dat:** 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 na nosiče informací, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování a likvidaci takových údajů.

- **Zpracovatel:** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

- **Citlivý osobní údaj:** osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo 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.

- **Souhlas 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.

3.2. Zkratky

- **GDPR:** (anglicky General Data Protection Regulation), 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 (obecné nařízení o ochraně osobních údajů), je nařízení Evropské unie, jehož cílem je výrazné zvýšení ochrany osobních dat občanů- obecné nařízení o ochraně osobních údajů

- **ICT:** informační a komunikační technologie

4. Odpovědnosti a pravomoci

- **Pověřenec pro ochranu osobních údajů**: poskytuje poradenství správci včetně jeho zaměstnanců, kteří provádějí zpracování osobních údajů, o jejich povinnostech podle GDPR; monitoruje soulad s GDPR a koncepcemi správce/zpracovatele v oblasti ochrany osobních údajů, poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování.
- **Správce ICT/správce sítě**: vede evidenci umístění instalačních médií a přehled o instalaci software na jednotlivé pracovní stanice a jeho kontrolách. Odpovídá za funkčnost a bezpečnost ICT.
- **Zastupitelstvo obce:** odpovídá za zajištění řádného vedení dokumentace, ochrany dat, autorských práv a používání legálního software.
- **Starosta obce:** odpovídá za informování veřejnosti o činnosti obce a za dodržování pravidel pro ochranu osobních údajů plynoucích z této Směrnice a z GDPR.
- **Zaměstnanec**: zaměstnanci vedou záznamy o činnostech zpracování pro jednotlivé účely zpracování v rozsahu své působnosti. Vedou evidenci souhlasů subjektů údajů v rámci svého předmětu činnosti včetně evidence subjektů údajů, které souhlas udělily. Hodnotí efektivitu a účinnost přijatých technických a organizačních opatření a realizuje jejich změny schválené starostou obce. Zaměstnanec obecně odpovídá za obsahovou správnost, kompletnost a následné uložení dat v okamžiku pořízení či změny dat, která pořídil či změnil bez ohledu na to, odkud byla data získána a v čí pracovní náplni je sběr a zpracování těchto dat. Dále odpovídá za dodržení ustanovení této Směrnice a souvisejících vnitřních předpisů.

5. Osobní údaje a jejich zpracování

5.1. Způsob zpracování osobních údajů

- Osobní údaje lze zpracovávat pouze za podmínek stanovených GDPR, případně zvláštními zákony, přičemž je nezbytné dodržovat ustanovení této Směrnice. Zpracovávat lze pouze osobní údaje získané zákonným způsobem.
- Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze osoby, kterými jsou:
  - zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů,
  - člen orgánu, pokud je to nezbytné pro výkon jeho funkce,
  - osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.

5.2. Účel zpracování, zákonnost

- Veškerá zpracování osobních údajů probíhají v rámci jednotlivých agend, tzv. „účelech zpracování".
- Právní titul - právním titulem je některé ustanovení čl. 6 odst. 1 písm. a) až f), čl. 9/2 písm. a) až j), čl. 10 GDPR. Ke každému účelu zpracování osobních údajů určí zaměstnanci právní titul účelu zpracování, který zaznamenají do Záznamů o

činnostech zpracování pro jednotlivé agendy. V případě, kdy agenda obsahuje i citlivé osobní údaje, určí zároveň právní titul pro citlivé údaje.

- Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu zpracování osobních údajů a navrhne nezbytný rozsah osobních údajů pro dané zpracování, dobu, způsob uchování a způsob informování subjektů údajů.
- Ke stanovení účelu zpracování osobních údajů a určení právního titulu si zaměstnanec vyžádá posouzení pověřencem.
- O každém nově zamýšleném účelu zpracování osobních údajů je ten, kdo navrhuje jeho účel, povinen informovat pověřence.
- Zaměstnanci jsou povinni 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 povinni dodržovat základní zásady při zpracování osobních údajů.

5.3. Zásady zpracování osobních údajů

Základní zásady při zpracování osobních údajů jsou:

- zpracovávat osobní údaje korektním a transparentním způsobem,
- před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování,
- zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu,
- zpracovávat osobní údaje přesně a podle potřeby je aktualizovat.

6. Informace o pověřenci pro ochranu osobních údajů

- Pro správce vykonává úkoly pověřence pro ochranu osobních údajů Bc. Nela Kubásková, e-mailová adresa: nelakubaskova@seznam.cz, telefon: +420 607 274 272
- Všichni zaměstnanci a osoby odpovědné za zpracování osobních údajů jsou povinni:
  - konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s GDPR,
  - poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování,
  - zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem.

7. Informace o právech subjektů údajů

Informaci o tom, jaké osobní údaje organizace správce zpracovává, si subjekt údajů může vyžádat na kontaktech uvedených na webových stránkách obce: www.statenice.cz.

8. Popis bezpečnostních opatření při ochraně osobních údajů

8.1. Obecné postupy při zabezpečení osobních údajů

- Přiměřeně zabezpečeny musejí být zpracovávané osobní údaje i ty, které nejsou systematicky zpracovávané, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech.
- 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 a dalších osobách:
  - na základě zákona o svobodném přístupu k informacím,
  - jsou veřejně dostupné (například ve veřejně přístupných registrech),
  - nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací.
- V pochybnostech je osoba odpovědná za zpracování osobních údajů vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.
- 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 osob odpovědných za zpracování osobních údajů zejména v uchovávání záznamových médií (písemných i elektronických), obsahujících osobní údaje, v uzamčených skříních nebo v uzamčených kancelářích a jiných míst a dále v dodržování pravidel informační bezpečnosti.
- Dále jsou osoby odpovědné za zpracování osobních údajů 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:
  - sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem,
  - hlasitě sdělovat osobní údaje ve veřejně přístupných prostorách,
  - umožnit nepovolaným osobám nahlížet do listin, které nesou osobní údaje, nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny,
  - sdělovat komukoliv svá přístupová hesla.

8.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje

- Písemnosti a digitální záznamová média, která obsahují osobní údaje, musí být mimo dobu, kdy jsou pod dohledem zaměstnanců, zabezpečeny v uzamčených skříních nebo v uzamčených kancelářích, popř. na jiných místech, zajišťujících jejich ochranu. To platí i pro kopie písemností a digitální zálohy, obsahující osobní údaje.
- Za plnění těchto povinností jsou odpovědny osoby zpracovávající osobní údaje podle rozsahu svých oprávnění.

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

- 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.
- Pevné počítače s přístupem k osobním údajům musejí mít alespoň zabezpečený přístup do počítače (přihlášení pod heslem) a při odchodu z kanceláře by měly být všechny počítače s přístupem k osobním údajům vypnuty.
- Také významné evidence osobních údajů (například mzdová, personální agenda, rozsáhlá evidence obyvatel a další) musejí být řádně zabezpečeny.
- Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložiště souborů mobilního telefonu a podobně, musejí být bezodkladně po přenosu bezpečně vymazána, pokud přenosné médium sloužilo jen k přenosu.
- Osoby odpovědné za zpracování osobních údajů pravidelně posuzují úroveň zabezpečení informačních systémů včetně přenosu dat s ohledem na rizika pro subjekty údajů, a v případě potřeby přijímají vhodná technická a organizační opatření, aby rizika zmírnily.
- Osoby odpovědné za zpracování osobních údajů zejména dbají na dostatečnou kvalitu hesel a pravidelné obměny hesel.

9. Porušení zabezpečení a míra jeho rizika

- Zjistí-li kdokoliv, že došlo k fyzickému nebo elektronickému porušení zabezpečení osobních údajů, například úniku, ztrátě, zničení, neoprávněnému zveřejnění osobních údajů (dále též pouze „incident"), neprodleně o tom informuje pověřence a starostu obce.
- Zaměstnanec vyhodnotí riziko pro práva a svobody subjektů údajů a výsledné stanovisko konzultuje s pověřencem. Pokud ve shodě s pověřencem posoudí jako nepravděpodobné, že by incident měl za následek riziko pro práva a svobody subjektů údajů (dále též pouze „nízké riziko"), provede o incidentu záznam k příslušnému účelu zpracování v záznamu o činnostech zpracování osobních údajů. Pokud vyhodnotí, že nejde jen o nízké riziko, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se zaměstnanec o porušení zabezpečení dozvěděl.
- Pokud je riziko pro práva a svobody subjektů údajů vysoké, zaměstnanec vhodným způsobem navíc informuje subjekty údajů.

10. Závěrečná ustanovení

- Kontrola dodržování Směrnice
  - Starosta obce zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice.
  - Starosta zajistí, aby byli s dokumentem Směrnice seznámeni všichni zaměstnanci. Prezenční listina o seznámení zaměstnanců se Směrnicí č. 01/2018 GDPR o ochraně osobních údajů je nedílnou součástí této Směrnice (viz příloha č. 1).
- Revize Směrnice
  - Revize Směrnice je provedena v případě potřeby, minimálně však jednou za dva roky.
  - Za zpracování, údržbu a revizi Směrnice odpovídá starosta obce.
  - Revize Směrnice se provádí na základě konzultace s pověřencem pro ochranu osobních údajů.

Ve Statenicích dne 19.12.2018

MgA. Apolena Novotná
Starostka obce

Příloha č. 1

Prezenční listina o seznámení zaměstnanců se Směrnicí č. 01/2018 GDPR o ochraně osobních údajů

Dne 10.12.2018 ve 14⁰⁰ h

Jméno	Příjmení	Funkce	Podpis
Mgr. ADOLENA	NOVOTNÁ	starostka	
Michal	POKORNÝ	místostarosta	
MIROSLAV	ŠANDA	místostarosta 2	
JANA	ŠPIČÁKOVÁ	info@statenice.cz	vedoucí úřadu starostky
Ing. ZUZANA	HANÁČKOVÁ	administrat.	
MIROSLAV	ŠANDA		