Směrnice č.1/2018
Ochrana zpracovávaných osobních údajů a dat a pokyny pro práci s IT

V souladu s ustanovením § 110 odst. (3) a odst. (4) písm. e) zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů (dále jen „zákon o obcích"), vydává starosta:
Obce Opatovec
IČ: 00579602
ADRESA: Opatovec 40, 568 02, Svitavy
tuto směrnici, která je závazná pro osoby a pracovníky Obecního úřadu Opatovec (dále jen „obecní úřad"):

1. Úvodní ustanovení a působnost

1.1. Na základě ustanovení § 248 a § 302 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, zákona č.101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, a Nařízení Evropského parlamentu a Rady (EU) 2016/679 (*dále jen „Nařízení GDPR")*, v platném znění je vydána tato směrnice upravující pravidla pro ochranu osobních údajů občanů Opatovce, zaměstnanců obecního úřadu a dalších fyzických osob, které mu byly poskytnuty k jeho využití.

1.2. Směrnice je v souladu se základními principy GDPR, kterými jsou: zákonnost, konkrétnost a transparentnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost, zodpovědný přístup a prokázání souladu.

2. Základní pojmy

V souladu Nařízením GDPR mají dále uvedené pojmy tento význam:
Osobním údajem je jakýkoli údaj, z něhož lze přímo či nepřímo zjistit identitu určité fyzické osoby – „**subjektu údajů"**, jakýkoli údaj týkající se této osoby.
Zvláštní kategorií údajů (dříve citlivé údaje) se rozumí osobní údaje takového charakteru, které mohou subjekt sám o sobě poškodit ve společnosti, v zaměstnání či jinde, nebo mohou zapříčinit jeho diskriminaci. Jedná se o údaje zahrnující informace o:

- národnostním, rasovém nebo etnickém původu,
- politických postojích, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích,
- náboženském či filozofickém přesvědčení,
- trestné činnosti,
- zdravotním stavu,
- sexuálním životě,
- jedinečných biometrických a genetických údajích.

Zpracování osobní údajů-jakákoliv operace s osobními údaji, jako je shromáždění, zaznamenání, uložení, pozměnění, nahlédnutí, použití, šíření, omezení, výmaz apod.
Správce osobních údajů-právnická nebo fyzická osoba (v tomto případě obecní úřad), která určuje účely a prostředky zpracování osobních údajů; zpracování provádí a odpovídá za něj.
Zpracovatel-fyzická nebo právnická osoba, orgán veřejné moci či jiný subjekt, který zpracovává osobní údaje pro správce (správce si jej najímá) na základě smlouvy. Zpracovatel plní stejné nároky na ochranu osobních údajů jako správce; může zpracovávat osobní údaje po technické stránce jen na základě přesných pokynů správce.

Pověřenec – osoba, která posuzuje činnost správce či zpracovatele, zda je v souladu s platnou právní úpravou, informuje je, radí, dává doporučení. Starosta obce jmenuje pověřence pro ochranu osobních údajů podle čl. 37 Nařízení GDPR (fyzickou, nebo právnickou osobu), uzavře s ním pracovně právní vztah, nebo smluvní vztah podle občanského práva.

3. Organizační opatření

3.1. Všichni zaměstnanci obecního úřadu jsou povinni dodržovat při shromažďování, evidenci a zpracování osobních údajů ustanovení výše uvedených zákonů a Nařízení GDPR, které mimo jiné stanoví, povinnosti při manipulaci.

3.2. Obecní úřad zajišťuje:

- úvodní proškolení všech zaměstnanců při nabytí účinnosti Nařízení GDPR;
- vstupní školení všech nových zaměstnanců při vzniku jejich pracovněprávního vztahu;
- periodická školení;
- ukončování pracovněprávního vztahu poučení zaměstnanců o tom, že jejich povinnosti při ochraně osobních údajů trvají i po ukončení pracovněprávního vztahu k organizaci;
- opatření při výskytu případů porušení zabezpečení osobních údajů;
- opatření při změně pravidel pro zabezpečení osobních údajů daných touto směrnicí, nebo zákony a nařízeními, na které se odkazuje;
- sleduje aktuální bezpečnostní situaci zpracování osobních údajů, potenciální hrozby ztráty nebo zneužití osobních údajů a pravidelně provádí testy zranitelnosti;
- evidenci všech osobních údajů shromažďovaných a zpracovávaných v obecním úřadem, tak aby byly shromažďovány pouze údaje skutečně nezbytné pro zajištění příslušných činností. Evidenci podléhají též osobní údaje osob, které jsou s obecním úřadem v kontaktu, např. uchazečů o zaměstnání, kontaktních osob či rodinných příslušníků tak, aby byla evidence úplná;
- uložení dokumentace s osobními údaji tak, aby se k dokumentaci dostaly pouze oprávněné osoby a bylo respektováno rozdělení pravomocí a odpovědností jednotlivých zaměstnanců, které odpovídají jejich pracovnímu zařazení (role);
- aktualizuje matici rolí, odpovědností a přístupů k osobním údajům.

3.3. Za plnění povinností podle bodu 3.2 odpovídá starosta obce.

3.4. Obsahem školení je zvyšování povědomí zaměstnanců zejména o tom, že:

- každý pracovník nese odpovědnost za ochranu zařízení jak na svém pracovišti, tak i mimo něj;
- musí být přijata adekvátní opatření pro ochranu osobních údajů v rámci fyzické ochrany;
- každý pracovník musí chránit své bezpečnostní a osobní údaje (hesla, kódy PIN, přístupové kódy apod.), nikomu je nesdělovat, hesla pravidelně měnit.;
- na zařízení smí být používán pouze podporovaný SW včetně operačního systému a internetového prohlížeče), musí být vždy bezprostředně aplikovány bezpečnostní update/patche a používat aktuální antivirové a anti-spyware programy s nastavenou on-line ochranou.;
- připojení přes internet je možné pouze prostřednictvím firewallu a pouze přes prověřená datová spojení včetně WI-FI sítí;
- z internetu a ani z jiných zdrojů se nesmí stahovat neznámé soubory, příp. programy;
- je nutné věnovat pozornost nedůvěryhodným e-mailům (zprávy od neznámých odesílatelů, případně zprávy s podezřelým názvem či obsahem), takové neotvírat a bez otevření mazat.
- je nutné ověřovat platnost certifikátu stránky;
- při jakémkoliv podezření na možnost zneužití svých přístupových údajů do služeb a na stránky, které uživatel používá, musí uživatel službu buď ihned zablokovat či změnit přístupové údaje;
- citlivá data včetně osobních údajů mohou být jen na schválených úložištích a zařízeních.

4. Pořizování a zacházení s údaji a daty

Obecní úřad shromažďuje a zpracovává osobní údaje v tomto rozsahu:

4.1. Na základě zákona, zejména

- souvisejí s pracovním a mzdovým zařazením zaměstnanců, se sociálním a zdravotním pojištěním;
- souvisejí s evidencí obyvatel obce;
- související s volbami;
- související s ochranou oprávněných zájmů obce (vymahatelnost pohledávek za dlužníky, záruční lhůty a pod).

4.2. Nad rozsah daný právními předpisy se souhlasem osoby, jejíž osobní údaje jsou zpracovány.
4.3. Odpovídající stanovenému cíli a rozsahu zpracování.
4.4. Pravdivé a přesné aktualizované osobní údaje.
4.5. Ke statistickým účelům jsou osobní údaje anonymizovány.

5. Práva subjektu údajů

5.1. Před samotným zpracováním osobních dat obecní úřad zajistí plnou informovanost těchto osob v rozsahu daném zákonem č. 101/2000 Sb., o ochraně osobních údajů a Nařízením GDPR. (vzor informace viz příloha č. 1,2,3 a 8)
5.2. Každý subjekt údajů má právo na opravu osobních údajů, které se ho týkají. Může se jednat o změnu adresy, jména, bydliště, telefonního čísla a podobně. Oprava se provede na základě doložení změny.
5.3. Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.
5.4. Subjekt údajů je oprávněn získat od obecního úřadu 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 souvisejícím následujícím informacím, a to na základě jeho žádosti a po prokázání jeho totožnosti.

6. Účelové omezení

6.1. Osobní údaje jsou shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely. Obecní úřad zpracuje přehled zpracovávaných osobních údajů a jejich účel v Soupisu funkcí a přístupů k osobním údajům (příloha č.5), který pravidelně aktualizuje. Obecní úřad vede evidenci udělených souhlasů se získáním a zpracováním osobních údajů v rozsahu minimálně jméno a příjmení, datum narození, druh osobního údaje, osobní údaj, účel, datum udělení, doba udělení souhlasu, odvolání souhlasu, výmaz.
6.2. Údaje pro různé účely nelze spojovat, musí být evidovány a zpracovány odděleně.
6.3. Osobní údaje zaměstnanců obecního úřadu jsou zpracovány za účelem splnění požadavků právních předpisů, zejména zákoníku práce (zpracovávané údaje spolehlivě a věrohodně prokazovaly vznik, průběh a ukončení pracovně právního vztahu zaměstnance, včetně poskytování platu), předpisů v oblasti sociálního zabezpečení, předpisů o archivaci a dále pro splnění povinností vůči třetím osobám (např. zdravotní pojišťovny, Česká správa sociálního zabezpečení, finanční úřad).
6.4. Osobní údaje uchazečů o zaměstnání zpracovává v rozsahu:
- nezbytné pro posouzení vhodnosti uchazečů (kvalifikace, zdravotní způsobilost).
- další rozšiřující informace až po případném rozhodnutí o uzavření pracovně právního vztahu.
- do rozhodnutí o uzavření pracovně právního vztahu; neúspěšným uchazečům jsou vráceny jimi zaslané dokumenty a jejich osobní údaje jsou vymazány.

7. Přístup k osobním údajům

7.1. Obecní úřad chrání shromážděné osobní údaje proti neoprávněnému přístupu.
7.2. Ke shromážděným osobním údajům mají přístup jen oprávnění zaměstnanci obecního úřadu uvedení v seznamu funkcí a přístupů (příloha č. 5). Ostatním zaměstnancům a osobám není přístup povolen s výjimkou osob k tomu oprávněných ze zákona.

7.3. Do osobního spisu zaměstnance mohou nahlížet starosta a místostarosta, účetní, orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby.

7.4. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele dle § 312 zákoníku práce.

8. Ochrana dat

8.1. 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 obecního úřadu, zamezí neoprávněnému přístupu k datům.

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

8.3. Všichni zaměstnanci přicházející do styku s provozními daty v listinné podobě a 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, požárem, živelní pohromou, a podobně.

9. Zásady pro manipulaci s listinnými dokumenty

9.1. Zaměstnanci, kteří pracují s listinnými dokumenty obsahujícími osobní údaje, jsou povinni uspořádat svou práci tak, aby tyto dokumenty byly po dobu práce stále pod jejich dohledem, aby byl znemožněn přístup neoprávněným osobám k těmto dokumentům.

9.2. Po ukončení práce s dokumenty obsahujícími osobní údaje, zaměstnanci uloží dokumenty do uzamykatelné skříně a při odchodu z pracoviště uzamknou místnost s uloženými dokumenty.

10. Zásady pro práci s výpočetní technikou

10.1. Je zakázáno:

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

10.2. Při zahájení práce s IT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěřené prostředky, tj. osobni počítače, tiskárny, modemy atd., vypnuty, s výjimkou těch zařízení, která musí zůstat s ohledem na své určeni trvale zapnuta.

10.3. Při ukončení nebo změně pracovně právního vztahu správce IT provede úpravu uživatelského účtu

zaměstnance, včetně přístupových práv dle pokynů starosty.

10.4. Počítačová (kybernetická) bezpečnost je zajišťována na všech počítačích obecního úřadu:

- instalací antivirových programů, firewallu;
- stanovením přístupových práv, hesel, zákazu sdílení hesel několika osobami;
- pravidelné zálohování dat, tak aby nedošlo k jejich ztrátě při případném odcizení či poruše počítače a byla zajištěna schopnost obnovy dat v případě fyzických či technických incidentů;
- zajištění automatických bezpečnostních aktualizací používaného software;
- pravidelné provádění testů zranitelnosti;
- při jakékoli likvidaci hardwaru musí být znemožněna možnost získání uložených osobních údajů;
- používání pouze silných hesel (heslo o délce minimálně osmi znaků, vždy musí jít o kombinaci malých a velkých písmen a čísel, případně zvláštních znaků);
- mazání a neotvírání nevyžádané pošty, odmazávání SPAM v emailové schránce i v počítačích;
- pravidelný servis výpočetní techniky je zaměřen i na kontrolu oblasti bezpečnosti dat, je prováděno pravidelné testování přijatých technických a organizačních opatření;
- pravidelným školením zaměstnanců v této oblasti.

11. Povinnost mlčenlivosti

11.1. Všichni zaměstnanci obecního úřadu a členové zastupitelstva, kteří se seznámili s osobními údaji uchovávanými obecním úřadem, jsou povinni o nich zachovávat mlčenlivost, a to i po skončení pracovního poměru nebo mandátu zastupitele (vzor ujednání o mlčenlivosti viz příloha č. 4).

11.2. Osobní údaje mohou být zaměstnancem v době trvání jeho pracovního poměru sděleny pouze subjektu údajů, kterého se týkají, a orgánům a institucím oprávněným ze zákona seznamovat se s osobními údaji.

12. Předávání osobních údajů

12.1. Osobní údaje se předávají zápisem do základních registrů.

12.2. Osobní údaje mohou být předány jen orgánům a institucím oprávněným ze zákona seznamovat se s osobními údaji.

13. Archivace a skartace

13.1. Osobní údaje jsou uchovávány pouze po dobu nezbytně nutnou pro účel jejich zpracování a po dobu skartační lhůty (viz Směrnice spisový a skartační řád).

13.2. Po dobu skartační lhůty se údaje uchovávají v listinné podobě nebo na technických nosičích. Dokumenty v listinné podobě jsou uloženy v uzamykatelné skříni kanceláře účetní a uzamčeném archivu. Technické nosiče jsou ukládány na obecním úřadu vždy v jiné místnosti než originální údaje. Zálohována jsou pouze všechna provozní data, nikoli software.

13.3. Na konci skartační lhůty elektronická i listinná data podléhají skartačnímu řízení. Dokumenty a data nevybrané jako archiválie se zničí, dokumenty a data vybraná příslušným státním archivem jako archiválie jsou předána tomuto archivu.

13.4. Dokumenty v elektronické podobě jsou ničeny:

- fyzickou destrukcí, jde-li o CD, DVD;

- použitím software zabezpečující vymazání, v tomto případě nesmí jít o pouhé smazání dokumentu, protože i poté by byla možná obnova smazaných souborů, musí jít o opakované přepsání původních souborů novými údaji.

14. Krizový plán

14.1. V případě poškození nebo ztráty vyměnitelného zálohovací zařízení je zaměstnanec povinen informovat starostu, který neprodleně informuje správce IT. Správce IT provede blokaci zařízení (např. mobilní telefon) a provede obnovu dat ze zálohy.

14.2. Starosta informuje pověřence, který splní oznamovací povinnost o možném úniku osobních údajů.

14.3. V případě zavirování zařízení – zaměstnanec neprodleně informuje starostu a správce IT. Správce IT provede odpojení napadeného zařízení od sítě a následně odviruje zařízení. Napadená data obnoví správce IT ze zálohy.

14.4. V případě napadení počítačové sítě zvenčí – správce IT odpojí server od sítě. Informuje pověřence pro možný únik osobních údajů. Správce IT prověří následky útoku a způsob útoku. Dále provede virovou kontrolu a přeheslování napadeného zařízení.

15. Závěrečná ustanovení

15.1. Tato směrnice je závazná pro všechny zaměstnance obecního úřadu, uživatele počítačového vybavení a pro osobu zajišťující činnosti správce IT. Starosta seznámí osoby, které nejsou zaměstnanci obecního úřadu, s touto směrnicí a povinností dodržovat její ustavení.

15.2. Směrnice nabývá účinnosti dnem 25. 5. 2018

V Opatovci

dne 23. 5. 2018

Martin Smetana
starosta obce