Obec Stará Lysá	
Směrnice č. 1/2023: Ochrana zpracovávaných osobních údajů a dat a pokyny pro práci s IT v organizaci	
Vypracoval:	Petr Vančík,
Schválil:	,
Směrnice nabývá platnosti ode dne:	1.3.2023
Směrnice nabývá účinnosti ode dne:	1.3.2023
Změny ve směrnici jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu.	

Úvodní ustanovení a působnost

Na základě zákona č. 110/2000 Sb. o zpracování osobních údajů, v platném znění, a Nařízení Evropského parlamentu a Rady (EU) 2016/679 (*dále jen „Nařízení GDPR“)*, v platném znění je vydána tato směrnice upravující povinnosti zaměstnanců organizace při ochraně dat zpracovávaných organizací a upravující pravidla pro ochranu osobních dat, zaměstnanců a dalších osob, které jsou s organizací v pracovněprávním nebo v jiném právním vztahu a dalších osob, které poskytují své osobní údaje organizaci k jejich využití. 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.

1. Základní pojmy

Osobním údajem je jakýkoli údaj, z něhož lze přímo či nepřímo zjistit identitu určité osoby.

Zvláštní kategorií údajů (dříve citlivé údaje) se rozumí 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 biologických rysech.

Zpracování osobní údajů – jakákoliv operace prováděná s osobními údaji, jako je shromáždění, zaznamenání, uložení, pozměnění, nahlédnutí, použití, šíření, omezení, výmaz apod.

Správce – právnická nebo fyzická osoba (v tomto případě obec), která určuje účely a prostředky zpracování osobních údajů.

Zpracovatel – fyzická nebo právnická osoba, nebo subjekt, který zpracovává osobní údaje pro správce (správce si jej najímá – např. mzdové účetnictví).

Pověřenec – osoba, která posuzuje činnost správce či zpracovatele, zda je v souladu s platnou právní úpravou, informuje je, radí, dává doporučení.

2. Organizační opatření

2.1. Všichni zaměstnanci a členové organizace jsou povinni dodržovat při shromažďování, evidenci a zpracování osobních údajů ustanovení výše uvedených zákonů a nařízení o ochraně údajů, které mimo jiné stanoví, co se těmito údaji a manipulací s nimi rozumí. Osobou ve obci zodpovědnou za ochranu osobních údajů je starosta/starostka.

2.2. Organizace zajišťuje:

- úvodní proškolení všech zaměstnanců při nabytí účinnosti směrnice GDPR;
- vstupní školení všech nových zaměstnanců při vzniku jejich pracovněprávního vztahu;
- periodická školení;
- opatření při výskytu případů porušení zabezpečení osobních údajů;
- opatření při změně pravidel pro zabezpečení osobních údajů daných touto směrnicí, nebo směrnicemi/zákony/nařízeními, na které se odkazuje;
- sleduje aktuální bezpečnostní situaci, potenciální hrozby a pravidelně provádí testy zranitelnosti ICT;
- evidenci všech osobních údajů shromažďovaných a zpracovávaných v organizaci, tak aby byly shromažďovány pouze údaje skutečně nezbytné pro zajištění příslušných činností. V evidenci osobních údajů má vypsané i typové osobní údaje, např. občanů, dobrovolníků či dárců, OÚ kontaktních osob či rodinných příslušníků, uchazečů o zaměstnání apod., 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 rolí zaměstnanců;
- a aktualizuje matici rolí, odpovědností a přístupů k osobním údajům;
- stanovení pravidel a procesů pro práci s osobními údaji tak, aby bylo minimalizováno riziko jejich zneužití, úniku, obecně možnost přístupu k nim neoprávněnými osobami.

Při ukončování pracovněprávního vztahu zaměstnanců jsou poučeni o tom, že jejich povinnosti při ochraně osobních údajů trvají i po ukončení pracovněprávního vztahu k organizaci.

2.3. 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, zároveň zodpovídá za zajištění odpovídajícího zabezpečení osobních údajů, se kterými přichází při výkonu práce do styku, tak aby se tyto údaje nedostaly do rukou nepovolaným osobám;
- 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, je musí uživatel službu buď ihned zablokovat či změnit přístupové údaje;
- citlivá data včetně osobních údajů mohou být jen na schválených úložištích a zařízeních.

3. Pořizování a nakládání s osobními údaji

3.1. Organizace shromažďuje a zpracovává pouze údaje, které

a) souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních partnerů, sociálním a zdravotním pojištění (např. dosažené vzdělání, délka praxe, funkční zařazení apod.), a to v souladu s platnými ustanoveními zákoníku práce,

b) souvisejí s aktivitami dle zákona o obcích a s návazným legislativním rámcem,

c) souvisejí s provozováním doplňkové činnosti,

d) souvisejí s organizováním veřejných akcí sportovně-kulturního charakteru,

3.2. Nad rozsah daný právními předpisy, pokud nejde o zpracování v oprávněném či veřejném zájmu je ke zpracování osobních údajů nutný souhlas osoby, jejíž osobní údaje jsou zpracovány. Před samotným zpracováním osobních dat organizace prokazatelně zajistí plnou

informovanost těchto osob v rozsahu daném Nařízením o ochraně OÚ a zákonem č. 110/2019 Sb. o zpracování osobních údajů. Poučení musí být zajištěno i v oblasti povinnosti zachování mlčenlivosti o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení zaměstnání nebo příslušných prací.

3.3. Pro statistické účely je třeba osobní údaje anonymizovat.

3.4. Lze shromažďovat a zpracovávat jen ty osobní údaje, které odpovídají stanovenému účelu a rozsahu zpracování. Ke zpracování se používají pouze pravdivé a přesné osobní údaje.

3.5. Každý subjekt osobních údajů má právo být informován o zpracování svých osobních údajů při shromažďování osobních údajů (tj. nejčastěji při prvním styku se správcem). Tím se rozumí právo na určité informace o zpracování jeho osobních údajů, tak aby byla naplněna zásada transparentnosti zpracování. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů. Správce osobních údajů je povinen tyto informace poskytnout, respektive zpřístupnit.

Mezi další práva subjektu údajů, patří:

a) právo na přístup k osobním údajům,
b) právo na opravu, resp. doplnění osobních údajů,
c) právo na výmaz,
d) právo na omezení zpracování,
e) právo na přenositelnost údajů,
f) právo vznést námitku,
g) právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování.

3.6. Zásady zpracování osobních údajů, mezi hlavní zásady zpracování osobních údajů patří tyto:

a) zákonnost, korektnost, transparentnost – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně,
b) omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
c) minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
d) přesnost – osobní údaje musí být přesné,
e) omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
f) integrita a důvěrnost – technické a organizační zabezpečení osobních údajů.

Jednotlivé zásady jsou detailně rozvinuty v článku 5 odst. 1 Obecného nařízení o ochraně osobních údajů.

4. Účelové omezení

4.1. Osobní údaje jsou organizací shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely.

4.2. Údaje pro různé účely nelze spojovat, musí být evidovány a zpracovány odděleně.

4.3. Rozsah zpracovávaných osobních údajů je stanoven v dokumentu „Informace o zpracování osobních údajů“, který je vyhotoven pro jednotlivé subjekty OÚ jejichž osobní údaje jsou zpracovávána (občané, zaměstnanci, uchazeči o zaměstnání, smluvní partneři apod.)

5. Přístup k osobním údajům

5.1. Je třeba zamezit neoprávněnému přístupu ke shromažďovaným osobním údajům.

5.2. K osobním údajům je povolen přístup pouze osobám, jejichž náplň práce tento přístup vyžaduje. Přesně je přístup k osobním údajům definován v tzv. matici rolí, která představuje přehled jednotlivých pracovních rolí, ke kterým je přiřazen rozsah osobních údajů, ke kterým je tato pracovní role oprávněna přistupovat.

5.3. Matice rolí definovaná v organizaci:

a) ***Starosta/starostka, zastupitelé, členové výborů a komisí*** mají v souladu se zákonem o obcích přístup ke všem informacím souvisejících s chodem obce ve vazbě na jimi vykonávanou činnost. Za dodržování zásad nahlížení do dat zodpovídá starosta/starostka.
b) ***Techničtí pracovníci (provoz, úklid)*** nemají právo nahlížet do dat vyjma aktivit souvisejících s jejich pracovní náplní
c) ***Sekretářka, asistentka, vybraní pracovníci*** mají právo pracovat s daty v souvislosti s charakterem vykonávané práce (vyřizování žádostí občanů, kontrolních, nadřízených, správních a dalších orgánů, poskytování informací, vyřizování stížností, vedení spisové služby apod.).

Všichni zaměstnanci, kteří vstoupí do kontaktu s kterýmikoliv osobními údaji nebo údaji zvláštní kategorie jsou povinni dodržovat mlčenlivost, a to i po případném ukončení pracovního poměru. To platí i pro třetí osoby, které mohou vstoupit s osobními daty klientů do kontaktu, proto mohou být osobní data poskytována pouze osobám, které mají mlčenlivost stanovenu zákonem či vyhláškou (například zaměstnanci obcí, krajů a státu, odborníci přizvaní k inspekci apod.), nebo je jejich mlčenlivost řádně ošetřena (například dodavatelé různých služeb) smluvním ujednáním nebo prostřednictvím podpisu písemného prohlášení o povinnosti mlčenlivosti.

5.4. K osobním údajům mají přístup také nadřízené, kontrolní a správní orgány, orgány soudní moci apod.

5.5. Příslušní vedoucí zaměstnanci, v jejichž působnosti se nachází dokumentace s osobnímu údaji, určí, v souladu s ustanovením Nařízení GDPR způsob nakládání s touto dokumentací.
5.6. 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.

6. Ochrana dat

6.1. 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 organizace. Přijatá opatření zamezí přístupu k datům nepovolaným osobám.

6.2. Předmětem ochrany jsou veškeré osobní údaje zpracovávané v 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.

6.3. 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, živelnou pohromou a podobně.

6.4. Obec při zpracovávání osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů, bezprostředně řeší každý bezpečnostní incident týkající se osobních údajů, a to v součinnosti s pověřencem pro ochranu osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, obec tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepíše záznam. O každém závažném incidentu obec informuje ve spolupráci s pověřencem Úřad pro ochranu osobních údajů.

7. Zásady pro práci s výpočetní technikou

7.1. 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 příslušného vedoucího pracovníka;
- provádět demontáž, úpravy, opravy, změny v nastavení a zapojení prostředků IT;
- používat prostředky IT pro jiné, než schválené účely;
- instalovat a hrát počítačové hry
- využívat soukromá zařízení (mobilní telefony, PC notebooky, tablety a další) pro pracovní účely a tato zařízení připojovat do sítě).

7.2. 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.

7.3. Při ukončení nebo změně pracovně právního vztahu vždy správce sítě provede úpravu uživatelského účtu pracovníka, včetně přístupových práv dle pokynů nadřízeného pracovníka.

7.4. Počítačová (kybernetická) bezpečnost je zajišťována na všech počítačích organizace:
- instalací antivirových programů, firewallu;
- stanovením přístupových práv, hesel, zákazu sdílení hesel několika osobami
- zákazem využívání funkce „zapamatování si hesla“;
- zákazem práce pod jiným než svým uživatelským účtem s přidělenými uživatelskými právy;
- 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 ICT;
- 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.

7.5. Jsou vyžívány následující bezpečnostní procedury:

- Ochrana autentizačních údajů (hesla), heslo není zobrazováno přímo, ale pomocí zástupných znaků;

- Přihlašovací informace je předávána mezi stanicí a serverem pomocí šifrované komunikace;
- Informační systém nepodává uživateli žádné informace o průběhu přihlašování, dokud není uživatel bezpečně a úspěšně přihlášen.

7.6. Pravidla elektronické výměny dat a informací

Jsou zavedeny procedury pro ochranu výměny informací (elektronická komunikace, použití hlasových a video komunikačních zařízení, případně též FTP) při splnění následujících bezpečnostních požadavků:

- Každý uživatel je poučen o možnostech kopírování, modifikací a zničení sdílených informací, případně o možnosti odposlechu neveřejných informací;
- Každý uživatel je obeznámen s postupy a nástroji pro detekci a ochranu před škodlivými kódy, které mohou být přenášeny elektronickou komunikací (antivirové programy);
- Uživatelé, osoby smluvních a třetích stran mají zodpovědnost (často smluvně garantovanou), že nezneužijí data, která si s obcí vyměňují například zasíláním reklamních sdělení, řetězovým zasíláním e-mailových zpráv apod.;
- Dokumenty, které obsahují osobní údaje, musí být bezprostředně po tisku odebírány z tiskárny či kopírky;
- Uživatelé jsou poučeni, aby v nezabezpečených webech nezadávali žádné osobní údaje, neveřejné informace a podobně.

7.7. Pravidla pro používání e-mailové komunikace

Přidělené schránky elektronické pošty (e-mailové schránky) s doménovým jménem obce smí být používány výhradně pro emailovou komunikaci související s výkonem práce.

Uvedené e-mailové schránky nesmí být používány pro odesílání nebezpečně (nešifrovaně) zabezpečených osobních údajů. Dále nesmí být služební e-mail využíván pro odesílání nelegálního obsahu (videa, hudba apod.) a soukromou korespondenci.

7.8. Pravidla pro používání informačních systémů

Práce s informačními systémy a v nich obsaženými osobními údaji se řídí zejména pokyny a nařízeními vedení obce. Uživatelé těchto informačních systémů a aplikací musí dbát především na dodržování následujících pravidel:

- Používat informační systémy výhradně k pracovním účelům;
- Používat přístupová hesla do informačních systémů a aplikací v souladu s pokyny pro používání hesel (viz výše).

7.9. Sledování událostí a audit síťových služeb a serverů

Na řadiči domény bude provedeno nastavení logování následujících událostí:

- Přihlášení do domény – úspěšné/neúspěšné;

- Lokální přihlášení – úspěšné/neúspěšné;
- Management uživatelských skupin a účtů – úspěšné/neúspěšné;
- Změny lokálních a doménových politik – úspěšné/neúspěšné;
- Privilegované operace – úspěšné/neúspěšné;
- Systémové události – úspěšné/neúspěšné.

Na dalších serverech je prováděno auditování stejných událostí jako na doméně, s výjimkou přihlášení do domény. Dále je logován přístup k informačním systémům, souborům a adresářům obsahujícím osobní údaje. Logovací údaje jsou na serverech uloženy po dobu **7** dní, poté jsou uloženy do centrálního úložiště logovacích souborů, kde jsou uchovávány minimálně po dobu **10** let. Archivaci logovacích souborů zajišťuje správce IT, pouze on má také ke všem bezpečnostním logům (zápis, smazání, čtení apod.) na serverech i v centrálním úložišti logů plný přístup.

8. Archivace a likvidace

8.1. Osobní údaje jsou uchovávány pouze po dobu nezbytně nutnou pro účel jejich zpracování a po dobu nezbytné archivace. Tato doba vychází zejména z platné legislativy (zákon o archivnictví, zákon o účetnictví a dalších)

8.2. Pro archivaci dat se v organizaci používá vyměnitelné zálohovací zařízení. Technické nosiče jsou uschovávány pouze na pracovištích organizace. Jsou ukládány vždy v jiné místnosti než originální údaje. Zálohována jsou pouze všechna provozní data, nikoli software. Účetní informace zálohují externí poskytovatelé těchto služeb na základě platných smluv.

8.3. Na konci úložní doby jsou elektronická i listinná data přezkoumána a odstraněna, pokud neexistuje oprávněný důvod pro jejich další uchování.

8.4. Listinné dokumenty jsou ničeny pomocí skartovacích kancelářských zařízení.

8.5. Dokumenty uložené 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.

9. Závěrečná ustanovení

Touto směrnicí jsou povinni se řídit v rámci svých pracovních povinností všichni zaměstnanci a rovněž další osoby, které jsou k organizaci v obdobném právním vztahu (zaměstnanci pracující formou dohody o práci konané mimo pracovní poměr, osoby spolupracující na základě smlouvy apod.).

Směrnice nabývá platnosti dnem:1.3.2023

Směrnice nabývá účinnosti dnem:1.3.2023

Ve Staré Lysé dne 1.3.2023

_____

Petr Vančík, starosta