Obec Radimovice, se sídlem Radimovice č. 47, 463 44 Sychrov	
Směrnice č. 3/2019 : Ochrana zpracovávaných osobních údajů a dat a pokyny pro práci s IT v organizaci	
Vypracoval:	Ondřej Zoubek, starosta obce Radimovice
Schválil:	Ondřej Zoubek, starosta obce Radimovice
Směrnice nabývá platnosti ode dne:	30.1.2019
Směrnice nabývá účinnosti ode dne:	30.1.2019
Změny ve směrnici jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu.	

Úvodní ustanovení a působnost

Na základě ustanovení § 248 a § 302 zákona č. 262/2006 Sb., zákoníku práce, v platném znění, zákona č. 101/2000 Sb. o ochraně 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 zpracovatelských organizací a upravující pravidla pro ochranu osobních dat zaměstnanců/klientů 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 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 obec), 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 - účetní, lékař) 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. Ředitel školy jmenuje pověřence pro ochranu osobních údajů podle čl. 37 nařízení (fyzickou, nebo právnickou osobu), uzavře s ním pracovně právní vztah, nebo smluvní vztah podle občanského práva.

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.

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. včetně stážistů, 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.

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;
- 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.

3. Pořizování a zacházení s údaji a daty

3.1. Organizace shromažďuje a zpracovává pouze údaje, které
- souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, a se sociálním a zdravotním pojištěním;
- související s poskytováním služeb klientů;
- souvisejí s identifikací pracovníka/klienta/dárců apod. v souladu se zákonem.

3.2. Nad rozsah daný právními předpisy je ke zpracování nutný souhlas osoby, jejíž osobní údaje jsou zpracovány. Před samotným zpracováním osobních dat organizace prokazatelně zajistí plnou informovanost těchto osob v rozsahu daném zákonem č. 101/2000 Sb., o ochraně osobních údajů a Nařízení GDPR. 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. Lze shromažďovat a zpracovávat jen ty osobní údaje, které odpovídají stanovenému cíli a rozsahu zpracování. Ke zpracování se používají pouze pravdivé a přesné osobní údaje.

3.4. Každý subjekt údajů má právo na opravu k osobním údajům, které se ho týkají. Může se jednat o změnu adresy, jména, bydliště, telefonního čísla a podobně.
3.5. Ke statistickým účelům je třeba osobní údaje anonymizovat.

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 osobních údajů zpracovaných o zaměstnancích organizace je dán požadavky právních předpisů, zejména zákoníku práce; je stanoven tak, aby zpracovávané údaje spolehlivě a věrohodně prokazovaly vznik, průběh a ukončení pracovně právního vztahu zaměstnance, včetně poskytování platu; dále splnění povinností vůči třetím osobám (např. zdravotní pojišťovny, Česká správa sociálního zabezpečení, finanční úřad) a předpisů o archivaci.

4.4. Rozsah osobních údajů zpracovaných o uchazečích o zaměstnání v organizaci

- Po uchazečích jsou vyžadovány pouze údaje nezbytné pro posouzení vhodnosti uchazečů v rámci výběrového řízení (kvalifikace, zdravotní způsobilost).
- Další rozšiřující informace jsou požadovány až po případném rozhodnutí o uzavření pracovně právního vztahu.
- Neúspěšným uchazečům jsou vráceny jimi zaslané dokumenty a jejich osobní údaje jsou vymazány.

5. Přístup k osobním údajům

5.1. Je třeba zamezit neoprávněnému přístupu ke shromažďovaným údajům.

5.2. K osobním údajům je povolen přístup pouze osobám k tomu zmocněným zákonem. Do osobního spisu zaměstnance mohou dále nahlížet vedoucí, jemu nadřízení pracovníci, orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Příslušní vedoucí zaměstnanci, v jejichž působnosti se nachází dokumentace s osobnímu údaji, určí v souladu s ustanovením Nařízení GDPR způsob s jejím nakládáním.

5.3. 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 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.

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, živelní pohromou, a podobně.

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.

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 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;
- 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.

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 ze zákona o archivnictví, zákona o účetnictví a dalších relevantních právních norem.

8.2. Pro archivaci dat se v organizaci používá vyměnitelné zálohovací zařízení/cloud. 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. Krizový plán

9.1. V případě poškození nebo ztráty vyměnitelného zálohovací zařízení/cloud je zaměstnanec povinen informovat vedoucího zaměstnance, který neprodleně informuje správce sítě nebo technického pracovníka. Ty dále informují **pověřence,** který splní oznamovací povinnost o možném úniku osobních údajů. Správce sítě nebo technický pracovník provede blokaci zařízení (např. mobilní telefon) a provede obnovu dat ze zálohy.

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

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

10. Závěrečná ustanovení

Ustanovení této směrnice jsou závazná pro všechny uživatele počítačového vybavení v rámci sítě a zaměstnance zajišťující činnosti správce sítě.

Kontrolou dodržování této směrnice je pověřen správce sítě a technický pracovník, který je zároveň kontaktní osobou externího správce sítě ve věci zajištění bezproblémového chodu a využívání počítačového vybavení v instituci.

Směrnice nabývá platnosti dnem: 30.1.2019

Směrnice nabývá účinnosti dnem: 30.1.2019

V Radimovicích dne 30.1.2019