**P r o t o k o l o i m p l e m e n t a c i**

**Obecného nařízení EU o ochraně osobních údajů č. 679/2016 (ON)**

**Obec TROUBKY-ZDISLAVICE, IČ 00287822**

1. **Průběh implementace**

Výsledek implementace je zachycen v tomto protokolu a v předaném **kontrolním záznamu**, v němž bylo identifikováno 35 jednotlivých účelů zpracování (agend). Kontrolní záznam byl předán objednateli a v průběžně aktualizované podobě slouží jako nástroj pro doložení souladu s ON,   
pro trvalé monitorování souladu s ON ze strany pověřence a pro řízení rizik při zpracování osobních údajů.

Pro zveřejnění informací na webu podle čl. 13 a 14 ON byla předána obecná textová informace (Informace o zpracování osobních údajů) a navazující sestava informací k jednotlivým agendám.

Záznamy o zpracování podle čl. 30 jsou součástí předaného kontrolního záznamu.

Součástí implementace byla také implementační schůzka dne: 6. 3. 2018

Jméno a funkce osob účastnících se implementační schůzky: Marie Šestáková, starostka

1. **Shrnutí výsledků implementace na základě kontrolního záznamu a implementační schůzky**
   1. **Zásadní zjištění (např. předávání osobních údajů neoprávněným osobám, neoprávněné zpracování osobních údajů bez právního titulu, nedostatečné zajištění citlivých osobních údajů, posílání rozsáhlého množství osobních údajů přes e-mail bez zabezpečení apod.):**
2. V pracovních smlouvách a dohodách o provedení práce/pracovní činnosti není dostatečně obsažena povinnost mlčenlivosti
3. Se zpracovateli dat (těmi, kteří s vašimi daty nakládají) není uzavřena smlouva nebo není v souladu s Obecným nařízením - formální nedostatky
4. Využívané souhlasy nejsou formálně v souladu s Obecným nařízením
5. Není dostatečně zajištěno zabezpečení přenosných médií
6. Není prováděna dostatečná záloha dat
7. Není dodržována lhůta uložení dokumentů a jejich skartace
8. V některých případech mohou být získávána data, které nesplňují zásadu minimalizace, tzn. jsou zjišťovány zbytečně nebo jsou zbytečně uloženy kopie dokladů (občanský průkaz, rodný list)
9. Elektronické soubory jsou zasílány emailem bez jakéhokoliv zabezpečení a tedy možnosti zcizení a zneužití
   1. **Méně závažná zjištění (např. souhlas se zpracováním, kde není nutný; nepořizování záloh, překročení doby uložení apod.):**
10. Do kanceláře není omezen přístup pro neoprávněné zaměstnance
11. Na stolech zůstávají dokumenty, které obsahují osobní údaje i v přítomnosti osob, které k nim nemají právo na přístup (uklizečka, návštěva)
12. V některých případech mohou být data využívána neoprávněně - jsou získány pro jiný účel zpracování
13. Na webových stránkách obce je archiv úřední desky s plnou verzí dokumentů
14. Webové stránky nejsou z hlediska GDPR dostatečně chráněny
15. **Doporučená nápravná opatření:** 
    1. **Prioritní (nutné realizovat v co nejkratším čase):**
16. Doplňte do vzoru pracovní smlouvy a dohod o provedení práce/ pracovní činnosti odstavec o povinnosti dodržování mlčenlivosti. Pro zapracování můžete využít zaslaný vzor SMS-služby, s.r.o.
17. Zajistěte, aby všechny vaše zpracovatelské smlouvy obsahovaly dle čl. 28: předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce, vč. mlčenlivosti
18. Každý souhlas musí být: svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná. Subjekt údajů má právo svůj souhlas kdykoli odvolat. Před udělením souhlasu o tom bude subjekt údajů informován (nejlépe na témže formuláři). Odvolat souhlas musí být stejně snadné jako jej poskytnout
19. U činností, které vyplývají z právních titulů uvedených v čl. 6 odst. 1 písmeno b-f (např. zákon, oprávněný zájem, smlouva..)  je získávání souhlasů nadbytečné a nesmí být zde získávány
20. Uchovávejte přenosná média (zvláště pokud je na nich záloha) zabezpečeně - uzamykatelná skříň, trezor. Nenechávejte stále připojená k PC a mějte nastavené šifrování média
21. Zaveďte dlouhodobý integrovaný a zabezpečený systém pro zálohu dat
22. Každý dokument je nutné uchovávat jen po dobu nezbytně nutnou. Po jejím uplynutí je nutno dokumenty skartovat nebo předat okresnímu archivu. Je nutné dbát na to, že skartace se týká i elektronických verzí dokumentů, které je nutné smazat
23. Nezjišťujte osobní údaje, pokud je nutně nepotřebujete. Jaké osobní údaje můžete zjišťovat udává v mnoha případech samotný zákon. Pokud neudává, zjišťujte raději méně, než více a nepořizujte si kopie dokladů
24. Pokud zasíláte dokumenty s osobními údaji emailem je nutné jistě vědět, kdo je na druhé straně emailu, dokument musí být chráněn - heslem (to je pak sděleno jinou formou, např. SMS), používat certifikát SSL či jiné zabezpečení
    1. **K postupnému řešení podle řízení rizik:**
25. Obecně je považováno za minimální ochranu 3 bezpečnostní opatření (např. vstupní dveře s bezpečnostním zámkem, uzamčena kancelář, uzamčené skříně, mříže na oknech a dveřích, kamerový systém, elektronický zabezpečovací systém…)
26. Je vhodné vést evidenci klíčů, mít přehled o tom, který zaměstnanec má přístup/klíče do budov či kanceláře
27. Do kanceláře má mít přístup jen osoba, čí kancelář je nebo oprávněná osoba, která má mít přístup k OsÚ v kanceláři. Je nutno mít zabezpečen PC vstupním heslem (min. 8 znaků, velké a malé písmena), které není snadno odhalitelné; nutno heslo aktualizovat; je doporučeno ho mít uchováno v listinné podobě na bezpečném místě
28. Není možné mít na nástěnkách či stolech a jiných viditelných místech volně napsána hesla a přístupové údaje k PC či využívaným softwarům, hesla a přístupové údaje musí být uzamčeny v trezoru nebo uzamykatelné skříňce
29. Ochrana osobních údajů začíná na stole, proto by se neměly volně zůstávat dokumenty s OsÚ na stolech apod., ale měly by být uloženy mimo dosah neoprávněných osob
30. Nezjišťujte osobní údaje, pokud je nutně nepotřebujete. Jaké osobní údaje můžete zjišťovat udává v mnoha případech samotný zákon. Pokud neudává, zjišťujte raději méně, než více a nepořizujte si kopie dokladů
31. Odstraňte nebo zaheslujte archiv elektronické úřední desky (důvod: např. na úřední desce je povinnost zveřejňovat obdržené dražební vyhlášky, exekuční příkazy bez anonymizace - po uplynutí povinné lhůty musí být dokument zanonymizován)
32. V případě, že se na webových stránkách vyskytují nějaké osobní údaje, aby byly zabezpečené - dostatečná ochrana je https://
33. **Další**
34. Zajistěte omezení přístupů k jednotlivým softwarům/programům v PC - každý zaměstnanec smí mít přístup jen tam, co spadá do jeho pracovní náplně
35. Projděte pracovní náplně zaměstnanců a přeformulujte co není jasně stanoveno, doplňte
36. Pokud využíváte email od společnosti Seznam, zvažte změnu poskytovatele, buď pod vlastní doménou nebo Google
37. Souhlas se zpracováním osobních údajů ve smlouvě je v rozporu s Obecným nařízením - zpracování údajů je dáno zákony /Zákoník práce, Zákon o účetnictví/ a tedy souhlas je nadbytečný a nesmí být vyžadován

Datum vystavení protokolu: 24. července 2018

Vystavila: Ing. Renata Bednářová