MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Metodické nástroje pro přípravu na obecné nařízení o ochraně osobních údajů

ISSS 2018

10. dubna 2018

Přehled metodických nástrojů

Ministerstvo vnitra průběžně zveřejňuje metodické nástroje, které jsou k dispozici obcím podle jejich konkrétní situace:

- **checklisty** pro malé obce,
- **systémové analýzy** – podávají návod na provedení analýzy rizik a nabízejí doporučená řešení modelových situací,
- metodika ke spisovým službám, vzorové dokumenty, metodika ke jmenování pověřence pro ochranu osobních údajů.

Hlavním účelem metodických nástrojů je poskytnout obcím podporu při přípravě na GDPR vlastními silami a ušetřit jim náklady na zbytečné externí služby.

Checklisty

Dokument je zamýšlen jako základní materiál, který má poskytnout počáteční orientaci odpovědných osob v malých obcích ohledně systémových požadavků obecného nařízení o ochraně osobních údajů. Jeho využití záleží na úvaze obce.

Obsahuje 3 základní listy

- "Úvod a doporučení",
- "Obecný seznam“, který obec provede po opatřeních, jimž je potřeba věnovat pozornost,
- "Seznam ke zpracování osobních údajů“, jenž lze využít při vlastní inventuře agend, kde se zpracovávají osobní údaje.

I. Nastavení kompetencí

V obci musí být určena osoba, která se věnuje níže uvedeným otázkám a zodpovídá za jejich řešení.
Má tedy odpovídající činnosti v popisu práce, popřípadě jí vyplývají z vnitřního předpisu nebo pokynu.

01. Stanovení prostředků (manuální/elektronické) zpracování osobních údajů.

02. Stanovení účelů zpracování (proč se údaje zpracovávají).

03. Posouzení, které osobní údaje je nutno shromažďovat.

04. Stanovení opatření, která omezí zpracování na minimální nutný rozsah.
(Např. nastavení kamery, základní dobu uložení údajů atd.)

05. Stanovení opatření, která prakticky chrání soukromí dotčených osob.
(Např. úroveň zabezpečení, rozsah sdělování příjemcům atd.)

06. Řízení přístupu - udělování oprávnění p

07. Poučení zaměstnanců o ochraně osobn

NOVĚ:

08. Jmenování pověřence pro ochranu oso

09. Zveřejnění kontaktních údajů pověřen

Metodiky k pověřenci:
Metodika Ministerstva vnitra
Pokyn pracovní skupiny WP 29 [evrops

Pověřence pro ochranu osobních údajů musí v souladu s obecným nařízením jmenovat každá obe
zaměstnance obce (nemusí být na celý úvazek, může vykonávat vedle činnosti pověřence i jiné
pověřence nakoupit od externího subjektu. Popřípadě může jednotlivý pověřence sdílet více obcí naj

Pověřenec poskytuje obci metodickou podporu, konzultace a školení a posuzuje soulad činnosti ob
osobních údajů. Je též kontaktní osobou pro Úřad pro ochranu osobních údajů.

Pověřenec nezodpovídá za ochranu osobních údajů, zodpovědná je obec jako správce. Pověřenec n
Nesmí být proto ve střetu zájmů - tedy nemůže současně stanovit systém ochrany osobních úd
Není však vyloučeno, aby plnil i jiné úkoly, které s funkcí pověřence nekolidují, zejména bude-li t
část úvazku dosavadního zaměstnance obce.

K podrobnostem viz metodiku Ministerstva vnitra: http://www.mvcr.cz/gdpr/soubor/metodicke-d
obci-k-organizacne-technickemu-zabezpeceni-funkce-poverence-pro-oou-dle-obecneho-narizeni-o-o
obci.aspx

NOVĚ:

10. Plnění povinnosti hlásit porušení zabezpečení ochrany osobních údajů ÚOOÚ.

Checklisty

Kontrolní seznamy pro jednotlivé agendy umožňují utřídit si základní informace o podmínkách zpracování osobních údajů v agendách, jejichž členění lze odvodit třeba z registru práv a povinností.
Checklist navede zpracovatele např. k revizi právních důvodů zpracování:

08.	Zpracování lze provést, neboť	a. dotčená osoba s tím souhlasila (zpravidla písemně)
		b. je nezbytné pro uzavření nebo plnění smlouvy
	(stačí jeden právní důvod)	c. je nezbytné pro plnění právní povinnosti obce
		d. je nezbytné pro ochranu životně důležitých zájmů osob
		e. je nezbytné pro plnění úkolu ve veřejném zájmu nebo pro výkon veřejné moci, kterým je obec pověřena
		f. je nezbytné k ochraně oprávněných zájmů obce nebo jiné strany, nad kterými nepřevažuje zájem dotčené osoby na svém soukromí

Checklisty

… nebo k revizi náležitostí smlouvy se zpracovatelem osobních údajů v příslušné agendě:

09.	Zpracování provádí pro obec externí zpracovatel:		
	a. ano		
		i. na základě právního předpisu	
		ii. na základě smlouvy, která upravuje (pokud to neupravuje právní předpis):	
			1. zapojení dalších zpracovatelů jen se souhlasem obce
			2. předmět a dobu zpracování
			3. povahu a účel zpracování
			4. typy osobních údajů a kategorie dotčených osob
			5. vázanost zpracovatele pokyny správce
			6. mlčenlivost osob provádějících zpracování u zpracovatele
			7. přijetí bezpečnostních opatření
			8. poskytování pomoci správci při plnění práv dotčených osob
			9. poskytování pomoci správci při plnění jeho povinností
			10. výmaz dat po skončení zpracování nebo jejich vrácení správci
			11. součinnost k doložení plnění povinností a při kontrolách a auditech
	b. ne		

Systémová analýza

! Provedení systémové analýzy není povinnost !

Obcím lze doporučit, aby před 25. květnem provedly inventuru zpracování osobních údajů. Jde však o doporučení postupu odpovídajícího praxi zodpovědného správce, nikoli o povinnost.

Složitost a forma inventury záleží na velikosti obce. Inventuru lze zvládnout vlastními silami. Navazovat by na ni měly úpravy vnitřních předpisů, revize souhlasů a zpracovatelských smluv, vždy dle potřeby a s možností využít vzorové dokumenty.

Lze ale využít i vzorovou analýzu, kterou MV v rámci své koordinační role nakoupilo pro využití obcemi.

Systémová analýza

Systémovou analýzu připravila Pražská znalecká kancelář, s.r.o. na vzorku 15 obcí.

Dokument je členěn na 2 bloky (pro obce 1. a 2. typu a pro obce s rozšířenou působností) a obsahuje:

- analýzu rizik,
- doporučená řešení modelových situací,
- vzorový časový plán přípravy na GDPR,
- přílohy, zejména přehled agend s uvedením právních titulů zpracování osobních údajů.

Analýza rizik

Analýza rizik vychází z metodologie používané v oblasti kybernetické bezpečnosti.

Identifikuje aktiva (úložiště, agendy, aplikace) a hodnotí jejich váhu.

Určuje hrozby a pro jednotlivá aktiva stanovuje jejich pravděpodobnost.

Určuje zranitelnost aktiv hrozbami.

Výsledkem je rizikové skóre.

Analýza rizik - aktiva

Listinné úložiště v rámci výkonu agend úřadu (L) – veškeré listiny, které jsou uloženy na úřadě a souvisí s výkonem agend úřadu;

Listinné úložiště v rámci vnitřního chodu úřadu (L) – veškeré listiny, které jsou uloženy na úřadě a souvisejí s vnitřním chodem úřadu (příjem a propuštění zaměstnanců, účetnictví atd.);

Informační systém spisové služby (E);

Agendové informační systémy – samostatná působnost (E);

Agendové informační systémy – přenesená působnost (E);

Ekonomický informační systém (E);

Portály – veřejné i neveřejné webové portály (E);

Ostatní elektronická úložiště (E) – e-mail, sdílené disky, lokální disky na počítačových sestavách.

Analýza rizik - hrozby

Příklad – pravděpodobnost hrozeb pro AIS v samostatné působnosti.

Vnější útoky	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Agendový informační systém u obcí se základním rozsahem je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které mají obce se základním rozsahem k dispozici.
Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla Zhotovitelem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS – samostatná působnost. Na obcích se základním rozsahem technické chyby nejsou častým jevem.
Lidský faktor	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Obce se základním rozsahem nemají pevně stanovené procesy prací s agendovými informačními systémy např. interními akty.
Narušení integrity OÚ	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obcích se základním rozsahem přenesené působnosti Zhotovitel nepředpokládá častější uplatnění dané hrozby.
Neoprávněný přístup	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení pravděpodobnosti uplatnění hrozby na nízkou úroveň. Přístupy do agendových informačních systémů jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.

Analýza rizik - hrozby

Příklad – AIS v samostatné působnosti - zranitelnost aktiva hrozbami.

Vnější útoky	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
Technické chyby	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
Lidský faktor	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
Narušení integrity OU	2	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla Zhotovitelem zvolena s ohledem na již dlouhou tradici AIS na obcích se základním rozsahem, kde jsou zaběhlé procesy využívání daného IS a u obcí se základním rozsahem nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
Neoprávněný přístup	3	Na základě zjištěných informací Zhotovitel přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední úroveň byla Zhotovitelem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS. Zároveň obce nedisponují aktivním řízením přístupů do AIS včetně monitoringu těchto přístupů.

Analýza rizik - skóre

Hodnota aktiva x pravděpodobnost hrozby x zranitelnost hrozbou.

Aktivum	Hodnota aktiva	Rizikové skóre								*Indikátor celkové míry rizika aktiva*
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů	
Listinné úložiště v rámci výkonu agend úřadu	5	30	15	60	45	30	30	60	60	330
Listinné úložiště v rámci vnitřního chodu úřadu	3	18	9	36	27	18	18	36	36	198
Informační systém spisové služby	5	20	50	30	40	20	45	60	45	310
Agendové informační systémy - samostatná působnost	5	20	40	40	30	45	45	45	45	310
Agendové informační systémy - přenesená působnost	5	30	20	20	40	45	30	30	45	260
Ekonomický informační systém	5	30	30	45	15	30	60	30	45	285
Portály	3	27	12	18	9	12	36	18	27	159
Ostatní elektronické úložiště	1	6	10	12	12	12	6	12	12	82
Indikátor celkové míry rizika hrozby	-	181	186	261	218	212	270	291	315	-

Modelová řešení

Systémová analýza obsahuje zásobu doporučení k řešení konkrétních situací. MV ji proto předložilo ÚOOÚ, který materiál v krátkém čase posoudil. Proběhlo jednání MV, ÚOOÚ a dodavatele. Po drobných úpravách a s jistou prodlevou byla analýza zveřejněna.

Diskuse s ÚOOÚ a dodavatelem se týkala například přístupu ke zveřejňování fotografií z obecních akcí. ÚOOÚ zastává právní názor umožňující poměrně pružná řešení. Neexistuje však ještě ustálená výkladová praxe.

Systémová analýza je proto opatrnější. Je možné, že praxe najde jednodušší řešení, nicméně analýza ukazuje bezpečnou cestu.

Jak systémovou analýzu používat

Jak používat systémovou analýzu:

- Nemá smysl ji pouze zkopírovat a prohlásit za svou. Doporučuje se seznámit se s analýzou a posoudit, které její části budou pro obec použitelné, a dále s nimi samostatně pracovat.
- Analýza rizik nezhodnocuje, kde je co špatně, ale ukazuje, jakou intenzitu zabezpečení vyžaduje to které úložiště, agenda nebo aplikace. Může ji zpracovat třeba pověřenec, ale není to povinnost.
- Modelové příklady – nabízejí se k volnému použití. Představují bezpečná řešení z hlediska GDPR s ještě únosnou mírou zátěže.
- V přílohách se zvlášť projevuje, že analýza vychází z dotazníků vyplněných vzorovými obcemi. Seznam agend lze využít při vlastní inventuře osobních údajů, ale je možné, že obec 1. stupně najde některou agendu třeba v příloze pro obce 2. stupně.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DĚKUJEME ZA POZORNOST