SMĚRNICE Č. 1/2018

O ŘÍZENÍ RIZIK

OBCE HVOZD

I.
Účel směrnice

1.1 Obec Hvozd, IČO: 00257826, se sídlem Hvozd 65, 331 01 Plasy (dále jen „Obec“) přijímá tuto směrnici z důvodu nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (dále též jen "GDPR").

1.2 Obec před přijetím této směrnice neměla upraveny interní procesy řízení rizik v souvislosti s ochranou osobních údajů fyzických osob.

1.3 Tato směrnice navazuje na čl. 24 GDPR tak, aby Obec mohla efektivně, včas a hospodárně předcházet rizikům ohrožujícím práva a svobody fyzických osob v oblasti ochrany osobních údajů.

1.4 Tato směrnice stanovuje interní postupy Obce ve věci řízení rizik spojených a souvisejících se zpracováním a nakládáním osobních údajů fyzických osob dle GDPR, jakožto i kompetence a odpovědnosti v systému řízení rizik.

II.
Definice základních pojmů

2.1 **Riziko** je nebezpečí, že určitá událost, jednání nebo stav nastane a bude mít negativní důsledek. Je definováno také jako pravděpodobnost vzniku události či změny, která nepříznivě ovlivní požadovaný výsledek. Je to přirozená vlastnost každé lidské činnosti. Odpovědní zaměstnanci musí stanovit, jakou míru rizika je možné tolerovat.

2.2 **Nežádoucí dopad** je výsledek působení rizika, který spočívá v narušení bezpečnosti osobních údajů fyzických osob při zpracování a nakládání Obcí. Může vést k neplnění stanovených úkolů a závazkových vztahů, příp. poškození dobrého jména Obce.

2.3 **Analýza rizik** je soustavná činnost, kterou jsou rizika vztahující se k činnosti Obce včas rozpoznávána a vyhledávána. Tato rizika jsou vyhodnocována a jsou o nich podávány informace příslušné úrovni řízení k přijetí rozhodnutí o tom, jak vyloučit nebo minimalizovat identifikovaná rizika nebo jejich nežádoucí dopady.

2.4 **Opatření** je popis konkrétní činnosti, která vede k odstranění, nebo aspoň ke snížení rizika.

III.
Kompetence k řízení rizik

3.1 V jednotlivých agendách spadá povinnost řídit rizika a odpovědnost za řízení rizik do působnosti příslušného vedoucího agendy Obce.

3.2 Vedoucí agendy Obce odpovídají v rámci svých kompetencí za:

a) včasné rozpoznávání a vyhledávání rizik v jimi řízené agendě
b) hodnocení stupně významnosti a určování priorit rizik
c) včasné oznámení skutečností o existenci významných rizik a předkládání návrhů zastupitelstvu Obce pro účely rozhodování a přijímání opatření k vyloučení nebo minimalizaci rizik
d) průběžné sledování identifikovaných rizik a včasnou reakci na nastalou bezprostřední hrozbu nežádoucího dopadu rizika
e) sestavení seznamu aktuálních rizik dle priorit
f) rozhodnutí k minimalizaci dopadů rizik
g) vedení dokumentace o řízení rizik
h) proškolování zaměstnanců v problematice rizik
i) pravidelné projednávání problematiky řízení rizik

3.3 Obec má následující agendy a následující vedoucí agendy:

a) Poskytování informací dle zákona č. 106/1999 Sb. – starosta
b) Czech Point – účetní
c) Katastr nemovitostí – účetní
d) Evidence obyvatel – účetní
e) Prezentace obce pro občany – starosta
f) Knihovna – knihovnice
g) Vedení obecní kroniky – kronikářka
h) Místní poplatky – starosta
i) Pronájmy obecních prostor – starosta
j) Spisová služba – místostarosta
k) Kácení stromů – místostarostka
l) Střet zájmů – místostarosta
m) Účetnictví – účetní
n) Evidence nálezců a majitelů nalezených věcí – starosta
o) Zákon o obcích – starosta
p) Stížnosti – místostarosta
q) Přidělení čísla popisného, evidenčního – místostarostka
r) Významné životní události občanů – místostarostka
s) Majetkoprávní transakce, kupní smlouvy – místostarosta
t) Smlouvy v lesním hospodářství – místostarosta
u) Emailová a telefonická komunikace s občany – starosta
v) Veřejné zakázky – místostarosta
w) Úřední deska – starosta
x) Hřbitovní poplatky – starosta

3.4 Povinností každého člena zastupitelstva Obce, účetní, zaměstnanců Obce je identifikovat a oznámit riziko včas vedoucímu příslušné agendy Obce.

IV.
Obecné zásady řízení rizik

4.1 Řízení rizik je systematická a metodická činnost organizovaná vedoucími zaměstnanci v rámci vnitřního řídícího a kontrolního systému tak, aby tento systém včas zjišťoval, vyhodnocoval a minimalizoval provozní, finanční, právní a jiná rizika vznikající v souvislosti s plněním schválených záměrů a cílů Obce.

4.2 Systém řízení rizik je součástí vnitřního řídícího a kontrolního systému, který je schopen hodnotit, řešit a snižovat dopady rizik hospodárným a účinným způsobem. Jedná se o neustálý proces. Měl by zahrnovat řízení všech rizik, která mohou ohrozit činnost úřadu. Aktivní řízení rizik zvyšuje mezi zaměstnanci povědomí o jejich existenci. Soustavný proces řízení rizik lze rozdělit do několika fází:

a) definování cílů, procesů, činností, postupů a konkrétních úkolů, které oddělení zabezpečuje
b) identifikace rizik (co by mohlo ohrozit naši práci, jak často a proč se to stává)
c) hodnocení rizik (hodnocení pravděpodobnosti výskytu a nežádoucího dopadu rizika)
d) řešení rizik (návrh opatření k předcházení, vyloučení nebo minimalizaci rizik)
e) následné prověření (kontrola účinnosti opatření ke zvládání rizik)

V.
Aktiva

5.1 Hodnocenými aktivy pro účely této směrnice jsou:

a) Listinné úložiště v rámci výkonu agendy úřadu – veškeré listiny, které jsou uloženy na úřadě a souvisí s výkonem agend úřadu.
b) Listinné úložiště v rámci vnitřního chodu úřadu – veškeré listiny, které jsou uloženy na úřadě a souvisejí s vnitřním chodem úřadu (příjem a propouštění zaměstnanců, účetnictví)
c) Agendové informační systémy – samostatná působnost – např. evidence poplatků
d) Agendové informační systémy – přenesená působnost – evidence obyvatel, volební agenda, legalizace, vidimace
e) Účetní a mzdový informační systém.
f) Portály – veřejné i neveřejné portály – např. stránky Obce
g) Ostatní elektronická úložiště – e-mail, datová schránka, sdílené disky, USB disky, lokální disky na počítačových sestavách.

VI.
Zdroje rizik

Hrozba	Popis
Vnější útoky	- zneužití přístupu k PC s možností neautorizovaného přístupu k osobním údajům nebo diskreditace osobních údajů; - krádež nebo prolomení hesla do obecního e-mailu, datové schránky nebo jiné aplikace s možností neautorizovaného přístupu - cílený útok na osobní údaje s motivem odcizení a neoprávněného užití s množností cílené diskreditace organizace - fyzické zcizení nebo poškození primárního aktiva včetně listinných evidencí s osobními daty - kompromitace dohledových prostředků nebo prostředků ke sledování a monitorování přístupu k osobním údajům - kompromitace identity oprávněného správce nebo zpracovatele
Technické chyby	- chyby zálohování - výpadek elektrické energie - výpadek hardwaru koncové stanice - výpadek softwaru koncové stanice - poškození nebo ztráta dat - mechanické poškození listinné evidence osobních údajů - narušení řádné čitelnosti listinné evidence osobních údajů - poškození/selhání programového vybavení - nedostatečné zabezpečení vstupů do míst, kde se nacházejí osobní údaje - nedostatečná údržba informačního systému nebo aplikace, kde jsou evidovány osobní údaje - nedostatečné postupy při identifikaci a odhalení incidentů - dlouhodobé přerušení podpory dodavatele SW
Lidský faktor	- obecná chyba uživatele - opomenutí uživatele - nedostatečné školení nebo povědomí o nakládání s osobními údaji nebo jejich ochrany - zkoušení prolomení uživatelem - poškození fyzické vrstvy sítě - zavlečení škodlivého SW - porušení bezpečnostní politiky uživatelem - zneužití oprávnění ze strany uživatelů - zneužití oprávnění ze strany administrátorů - narušení fyzické bezpečnosti – kancelář, serverovna - nepřítomnost/zranění/smrt administrátora IS - nedostatečné vymezení bezpečnostních pravidel - nedostatečná míra nezávislé kontroly - nedostatečná ochrana úložišť listin obsahující osobní údaje

Narušení integrity osobních údajů	- neoprávněné manipulování evidencemi osobních údajů na úrovni informačního systému nebo aplikací pod správou správce - neoprávněné manipulování s listinnými evidencemi obsahujícími osobní údaje - provedení neoprávněných činností - zneužití vedených osobních údajů - nevhodné či nesprávné nastavení přístupových oprávnění - fyzické narušení listiny obsahující osobní údaje
Neoprávněný přístup	- k osobním údajům má přístup osoba, která k danému úkonu nemá oprávnění - modifikace vedených osobních údajů - nedostatečné monitorování činnosti uživatelů - nedostatečné monitorování činnosti administrátorů
Narušení dostupnosti	- nedostupnost osobních údajů z důvodu pochybení organizačního charakteru - nedostupnost osobních údajů z důvodu technického pochybení
Ztráta osobních údajů	- nevhodná manipulace s listinnou evidencí obsahující osobní údaje - technické chyby v informačním systému uchovávající osobní údaje - úmyslné zcizení osobních údajů v listinné podobě z listinné evidence - úmyslný export osobních údajů z informačního systému nebo aplikací - výmaz osobních údajů z informačního systému nebo aplikací - předání listinné evidence osobních údajů neautorizované osobě bez udání důvodů a bez dostatečné evidence povinnosti navrátit předané osobní údaje
Narušení práv a svobod soukromí subjektu údajů	- narušení práva na soukromí - narušení práva na ochranu cti a důstojnosti - narušení práva na informační sebeurčení - narušení práva na život - narušení práva na duševní a tělesnou integritu - narušení práva subjektu údajů na informace a přístupu k osobním údajům - narušení práva subjektu údajů na výmaz (právo být zapomenut) - narušení práva subjektu údajů na omezení zpracování osobních údajů

	- narušení práva subjektu údajů na přenositelnost osobních údajů - narušení práva na ochranu osobních údajů - úmyslná kompromitace osobních údajů třetím subjektem - narušení zákazu diskriminace - narušení ochrany identity - hmotné ztráty subjektu údajů - neoprávněné zrušení pseudonymizace

VII.
Hodnocení pravděpodobnosti rizika

Stupeň	Četnost výskytu	Kritérium
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo nulové.
2	Nízká	Hrozba se může uplatnit méně než 1x za rok, nebo kritické období.
3	Střední	Hrozba se může uplatnit zhruba 1x za rok, resp. hrozba se jednou uplatnila v průběhu kritického období.
4	Vysoká	Hrozba se může uplatnit zhruba 1x za měsíc, resp. hrozba se jednou uplatnila v průběhu více něž 1x v kritickém období.
5	Velmi vysoká	Hrozba se může uplatnit zhruba 1x týdně, resp. hrozba se uplatnila denně v kritickém období.

VIII.
Identifikace zranitelnosti

Stupeň	Zranitelnost aktiva	Kritérium
1	Velmi nízká	Hrozba se nemůže vůči aktivu uplatnit
2	Nízká	Aktivum je chráněno, resp. je odolné velmi dobře proti uplatnění hrozby
3	Střední	Aktivum je chráněno částečně, resp. je mírně odolné proti uplatnění hrozby.
4	Vysoká	Aktivum je chráněno, resp. je odolné velmi nedostatečně proti uplatnění hrozby.
5	Velmi vysoká	Aktivum není chráněno vůbec.

IX.
Stupnice hodnocení aktiv

Stupeň	Hodnota	Kritérium
1	Velmi nízká	Ztráta, poškození, narušení bezpečnosti primárního aktiva má jen nepatrný nebo žádný vliv na ochranu osobních údajů v rámci organizace Obce. Z pohledu GDPR obsahuje aktivum osobní údaje zaměstnanců obce či úřadu.

2	Nízká	Ztráta, poškození, narušení bezpečnosti primárního aktiva má nízký dopad na zákonné povinnosti Obce v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci GDPR.
3	Střední	Ztráta, poškození, narušení bezpečnosti primárního aktiva má střední dopad na zákonné povinnosti Obce v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností nebude mít zásadní vliv na fungování organizace Obce jako celku. Z pohledu GDPR obsahuje aktivum osobní údaje občanů.
4	Vysoká	Ztráta, poškození, narušení bezpečnosti primárního aktiva je velmi významná, může vést k neakceptovatelnému porušení zákonných požadavků v rámci ochrany osobních údajů. Narušením primárního aktiva pravděpodobně dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít vliv na fungování organizace Obce jako celku.
5	Velmi vysoká	Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace Obce. Z pohledu problematiky GDPR aktivum obsahuje citlivé osobní údaje.

X.
Celková míra rizika a řešení rizik

10.1 Ohodnocení míry rizika se provádí součinem hodnoty aktiv, pravděpodobnosti rizika a zranitelnosti, tj. tzv. rizikovým skórem, které se pohybuje v rozmezí 1-125 bodů. Hranice akceptovatelného rizika je předmětem manažerského rozhodování na straně Obce.

10.2 V rámci Obce není zřízeno oddělení interního auditu osobních údajů, působnost v této oblasti má kontrolní výbor zastupitelstva Obce. Kontrolní výbor Obce provádí nezávislé hodnocení, zda je systém řízení rizik v Obci přiměřený a funkční. Na základě těchto individuálních šetření poskytuje vedoucím agend doplňující informace o výskytu a úrovni rizik.

10.3 Podle svého postoje k rizikům může vedoucí agendy v řízení rizik činit následující:

a) **riziku se vyhýbat**, například tím, že činnost kde riziko vzniká, nebude vykonávat nebo odstraní příčinu rizika
b) **riziko kontrolovat**, například tím, že činnost kde riziko vzniká, bude obsahovat kontrolní mechanismus, který riziko sníží

c) **riziko sdílet**, znamená, že riziko z prováděné činnosti ponesou spolu s vedoucím agendy další vedoucí agend
d) **riziko převádět** znamená, že riziko z prováděné činnosti subjekt převede na jinou organizaci (např. na pojišťovnu)
e) **riziko sledovat** jako nevyhnutelné se současným přijetím opatření, pokud riziko nastane
f) **riziko přijmout** bez jakýchkoliv opatření v případě, že je pro Obec na přijatelné úrovni

10.4 Vedoucí agendy v případě vzniku rizika informuje zastupitelstvo Obce o vzniku rizika a o způsobu řešení rizika. Zastupitelstvo Obce je oprávněno změnit způsob řešení rizika přijatý vedoucím agendy.

XI.
Závěrečné ustanovení

Tato směrnice byla schválena na zasedání zastupitelstva Obce Hvozd konaného dne 21.05.2018 a nabývá platnosti a účinnosti dne podpisu starosty a místostarosty Obce.

Ve Hvozdě dne 21.05.2018

Daniel Reiprich, starosta

Mgr. Jan Lego, Ph.D., místostarosta