

Analýza rizik zpracování osobních údajů

(aktualizace dle GDPR a zákona č. 110/2019 Sb.)

1. Úvodní ustanovení

Tento dokument „Analýza rizik zpracování osobních údajů“ (dále jen „analýza rizik“) je zpracován v souladu s:

- Nařízením Evropského parlamentu a Rady (EU) 2016/679 (GDPR),
- zákonem č. 110/2019 Sb., o zpracování osobních údajů,
- souvisejícími právními předpisy České republiky.

Dokument nahrazuje předchozí znění analýzy rizik a představuje její **kompletní revizi a aktualizaci** s cílem zajistit soulad se současnými požadavky na ochranu osobních údajů a principem odpovědnosti (accountability).

2. Správce osobních údajů

Správce: Obec Hory

Správce zpracovává osobní údaje při výkonu samostatné i přenesené působnosti, dále v postavení zaměstnavatele, smluvní strany a při výkonu dalších zákonných činností.

Správce vystupuje v postavení správce osobních údajů ve smyslu čl. 4 odst. 7 GDPR, neboť určuje účely a prostředky zpracování osobních údajů, případně mu jsou tyto určeny právními předpisy.

3. Účel a význam analýzy rizik

Účelem této analýzy je:

- identifikovat rizika pro práva a svobody subjektů údajů,
- posoudit pravděpodobnost a dopady těchto rizik,
- stanovit a popsat technická a organizační opatření přijatá správcem,
- prokázat soulad zpracování osobních údajů s GDPR.

Analýza je zpracována **přiměřeně rozsahu, povaze a účelům zpracování**, s ohledem na velikost obce a charakter vykonávaných činností.

4. Metodika řízení rizik

Řízení rizik vychází zejména z čl. 24, 25 a 32 GDPR.

Riziko je hodnoceno jako kombinace:

- **pravděpodobnosti** jeho výskytu,
- **dopadu** na práva a svobody subjektů údajů.

Stupnice hodnocení

- Pravděpodobnost: nízká / střední / vyšší
- Dopad: nízký / střední / závažný

Výsledkem je celkové hodnocení rizika jako:

- nízké,
- střední,
- vyšší.

Správce nepoužívá absolutní tvrzení o neexistenci rizik, ale pracuje s jejich **přiměřeným řízením**.

5. Přehled zpracování osobních údajů

Správce zpracovává osobní údaje zejména na základě:

- čl. 6 odst. 1 písm. c) GDPR – plnění právní povinnosti,
- čl. 6 odst. 1 písm. e) GDPR – výkon veřejné moci a veřejného zájmu,
- čl. 6 odst. 1 písm. b) GDPR – plnění smlouvy,
- výjimečně čl. 6 odst. 1 písm. a) GDPR – souhlas subjektu údajů.

Správce nezpracovává osobní údaje ve velkém rozsahu ani systematicky zvláštní kategorie osobních údajů, s výjimkou zákonem stanovených případů (např. pracovněprávní agenda).

6. Technická a organizační opatření

6.1 Technická opatření

- řízení přístupů k informačním systémům (individuální přihlašovací údaje),
- zabezpečení pracovních stanic heslem,
- pravidelné aktualizace software,

- antivirová ochrana a firewall,
- pravidelné zálohování dat,
- omezení používání přenosných médií.

6.2 Organizační opatření

- omezení přístupu k osobním údajům pouze oprávněným osobám,
- uzamykání kanceláří a listinných spisů,
- vnitřní pravidla pro nakládání s dokumenty,
- mlčenlivost osob přicházejících do styku s osobními údaji,
- pravidelné školení zaměstnanců.

6.3 Řešení bezpečnostních incidentů

Správce má nastaven postup pro:

- identifikaci bezpečnostního incidentu,
 - posouzení jeho dopadu,
 - dokumentaci incidentu,
 - případné oznámení ÚOOÚ dle čl. 33 GDPR.
-

7. Vyhodnocení rizik podle agend

Níže uvedené agendy představují hlavní oblasti zpracování osobních údajů u správce.

7.1 Mzdová a personální agenda

- Právní titul: čl. 6 odst. 1 písm. c) GDPR
- Riziko: střední (citlivost údajů)
- Opatření: omezený přístup, zabezpečení listinné i elektronické podoby

7.2 Smluvní agenda

- Právní titul: čl. 6 odst. 1 písm. b) a c) GDPR
- Riziko: nízké
- Opatření: kontrola zveřejňovaných údajů, archivace dle spisového řádu

7.3 Účetnictví a daňové doklady

- Právní titul: čl. 6 odst. 1 písm. c) GDPR
- Riziko: nízké
- Opatření: omezený přístup, zákonné lhůty uchování

7.4 Evidence obyvatel

- Právní titul: čl. 6 odst. 1 písm. c) GDPR

- Riziko: střední
- Opatření: přístup pouze oprávněným osobám, zabezpečení evidence

7.5 Ostatní správní agendy

- Riziko: nízké
 - Opatření: standardní organizační a technická opatření
-

8. Pověřenec pro ochranu osobních údajů

Správce má jmenovaného pověřence pro ochranu osobních údajů v souladu s čl. 37 GDPR.

Pověřenec:

- monitoruje soulad zpracování s GDPR,
 - poskytuje poradenství,
 - spolupracuje s dozorovým úřadem,
 - je kontaktním místem pro subjekty údajů.
-

9. Závěrečné zhodnocení

Na základě provedené analýzy správce konstatuje, že:

- zpracování osobních údajů je prováděno zákonně, transparentně a přiměřeně,
- přijatá technická a organizační opatření odpovídají míře rizik,
- nebyla identifikována zpracování vyžadující posouzení vlivu dle čl. 35 GDPR.

Správce se zavazuje:

- průběžně aktualizovat tuto analýzu,
 - reagovat na změny právních předpisů a procesů,
 - dále posilovat ochranu osobních údajů.
-

Tato analýza rizik je platná dnem schválení a nahrazuje předchozí verze.