Obec Brambory

Směrnice pro zpracování a zabezpečení osobních údajů

Obsah **Str.**

2 POJMY

Pojem/zkratka	Výklad
Hrozba	Jakákoliv okolnost či událost, která může potenciálně využít zranitelné místo procesu zpracování osobních údajů (agendy) a způsobit škodu
Informační aktiva	Pro účely tohoto dokumentu jsou za informační aktiva považovány všechny osobní údaje a další informace, které pro Obec přímo představují hodnotu, a narušení jejich bezpečnosti může mít pro Obec negativní dopad
Proces zpracování osobních údajů Obce / PZOÚ	Proces, ve kterém se na předem definovaný nebo stanovený účel systematicky zpracovává, nebo má zpracovávat jakýkoliv uspořádaný soubor osobních údajů, přístupných podle určených kritérií, bez ohledu na to, zda jde o systém centralizovaný, decentralizovaný nebo distribuovaný na funkčním nebo geografickém základě; procesem se pro účely tohoto dokumentu rozumí také soubor osobních údajů, které jsou zpracovávány nebo připraveny na zpracovávání částečně automatizovaných nebo jinými než automatizovanými prostředky zpracování (manuální, poloautomatizované)
Pověřenec pro ochranu osobních údajů	Marie Francová mikroregioncaslavsko@gmail.com
IT služba	Služba poskytovaná provozem IT útvaru Obce (interní nebo externí útvar)
Kamerový systém / KS	Kamerovým systémem se pro účely tohoto dokumentu rozumí využití dostupných technických prostředků ke generování/snímaní obrazu, přenosu obrazu a zobrazení obrazu, případně společně obrazu se zvukem (např. CCTV, tzv. fotopasti, webkamery apod.), pokud se tyto obrazy ukládají na záznamové médium (nosič)
Malware	Škodlivý kód (Malware) je počítačový kód, který způsobuje narušení zabezpečení údajů (informací) za účelem poškození počítačového systému. Výraz "Malware" pochází ze spojení dvou anglických slov Malicious (škodlivý) a software (software)
Oprávněná osoba	Každá fyzická osoba, která přichází do styku s osobními údaji v rámci svého pracovního poměru, zaměstnaneckého poměru k Obci, služebního poměru, členského vztahu, na

Přijatelné riziko	Přijatelné riziko je riziko, které je tak nízké, že pro Obec nepředstavuje významný negativní dopad a není nutné uplatnit další opatření k jeho snížení, minimalizaci
Zbytkové riziko	Zbytkové riziko je riziko, na které byly uplatněny všechna dostupná opatření na komplexní ošetření rizik, tj. byla implementována základní, dodatečná a vylepšená opatření na ošetření rizika
Ošetřování rizika	Jeden ze tří sub-procesů procesu řízení rizik (analýza rizik, ošetřování rizika a přehodnocování rizik), v rámci kterého jsou přehodnocovány doporučené technické, organizační a procedurální protiopatření. Následně jsou těmto protiopatřením stanoveny priority implementace
Příjemce	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování (článek 4 GDPR)
Pseudonymizace	Zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě
Správce	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Pro účely tohoto dokumentu je správcem Obec (článek 4 GDPR)
Subjekt údajů	Fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby (článek 4 GDPR)
Třetí strana	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající

Obec a každá její složka, počínaje řídícími pracovníky přijala závazek brát ohled na bezpečnostní požadavky zúčastněných stran při budování bezpečného prostředí, včetně všech provozních oblastí a při šíření cílů, hodnot a poznatků společných pro celou Obec.

Prosazování základních bezpečnostních principů v každodenní činnosti Obce je trvalý, cílevědomě řízený a organizovaný proces v metodické, výkonné a kontrolní oblasti.

Základním bezpečnostním cílem je zajistit osobní údaje a ostatní citlivá informační aktiva Obce proti odcizení, ztrátě, poškození, zničení, kompromitaci, neoprávněnému nebo nedovolenému přístupu, zpřístupnění neoprávněným osobám, neoprávněné změně a neoprávněnému rozšiřování a před jakýmikoli nepřístupnými a zlomyslnými formami zpracování. Pro tento účel Obec přijímá odpovídající technické, organizační a personální opatření, jejichž funkčnost se bude překrývat a vytvářet integrovanou ochranu celého procesu zpracování osobních údajů.

Obec se zavazuje implementovat zejména následující bezpečnostní funkce:

- zajištění dostupnosti citlivých informačních aktiv („dostupnost údajů"),
- zajištění integrity citlivých informačních aktiv („integrita údajů"),
- zajištění důvěrnosti citlivých informačních aktiv („důvěrnost údajů"),
- relevantní prokázání odpovědnosti a sledovatelnost přístupu k citlivým informačním aktivům („zásada odpovědnosti").

Bezpečnostní politika Obce zahrnuje oblast fyzické i informační bezpečnosti pomocí technických opatření, organizačních opatření a personálních opatření.

Ustanovení tohoto dokumentu se vztahují na všechny útvary, které se podílejí na veškerých aktivitách Obce.

Při změně bezpečnostní politiky, technických opatření, organizačních opatření nebo personálních opatření, při změně používaných informačních systémů a/nebo jejich konfigurace a/nebo jejich umístění, nebo při změně obecně závazných právních předpisů České republiky nebo legislativy Evropské Unie se Obec zavazuje Směrnici neprodleně upravit a doplnit potřebné změny.

3.2 Politika řízení rizika

Řízení rizik v procesu zpracování osobních údajů je systematický proces, ve kterém se identifikují a analyzují hrozby a zranitelnosti a posuzuje se míra rizika, souvisejícího se zpracováním osobních údajů, s pořízením, dodávkou, či vývojem aplikací a informačních systémů, se zpracováním, přenášením a ukládáním informací pomocí IT prostředků, a kterým se definuje optimální způsob ošetření rizika při minimálních finančních a časových nákladech a respektování strategických cílů Obce.

Úkolem managementu rizik je především dosažení přiměřené bezpečnosti a ochrany informačních aktiv, vypracováním optimální strategie řízení rizik, jak hlavních nositelů možných budoucích škod.

Řízení rizik v bezpečnosti procesu zpracování osobních údajů musí splňovat následující požadavky:

- jsou identifikovány hrozby a zranitelnosti a jsou stanoveny míry rizik,

- je formálně deklarován závazek vedení Obce řídit a snižovat bezpečnostní rizika,
- je zaručena účast řídících zaměstnanců na programu řízení rizik,
- je formálně stanoven tým zodpovědný a odborně zdatný správně identifikovat bezpečnostní rizika, jakož i aplikovat metodiku hodnocení rizik na specifické činnosti či IT systémy,
- je zaručena plná podpora a účast zaměstnanců zodpovědných za informační technologie na řízení rizik,
- je zajištěna konzistence výsledků jednotlivých analýz rizik a jednotný pohled na zjištěná rizika, a to bez ohledu na to, jaký přístup a metodika byly zvoleny při výkonu jednotlivých dílčích analýz rizik,
- je neustále zvyšováno povědomí a spolupráce uživatelů při dodržování procesů a udržování souladu s implementovanými opatřeními,
- je zaručen nepřetržitý proces oceňování a hodnocení IT rizika.

3.5 Zásady ochrany osobních údajů

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokalizační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Osobní údaje, zpracovávané Obcí jsou:

- ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem (**zákonnost, korektnost a transparentnost**),
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nejsou dále zpracovávány způsobem, který je s těmito účely neslučitelný (**omezení účelem**),
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (**minimalizace údajů**),
- přesné a v případě potřeby aktualizované; Obec přijala veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny (**přesnost**),
- uloženy ve formě, umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (**omezení uložení**),
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (**integrita a důvěrnost**).

S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavedla Obec vhodná technická a organizační opatření, aby zajistila a byla schopna doložit, že

- nepřetržitá přítomnost oprávněné osoby v chráněném prostoru, pokud se v něm nacházejí i jiné než oprávněné osoby,
- režim údržby a úklidu chráněných prostor Obce,
- pravidla manipulace s fyzickými nosiči osobních údajů (např. listiny, fotografie) mimo chráněných prostor a vymezení odpovědnosti,
- pravidla užívání automatizovaných prostředků zpracování (např. notebooky) mimo chráněné prostory Obce a vymezení odpovědnosti.

3.8 Právní základ zpracování osobních údajů

Právním základem zpracování osobních údajů Obce jsou zejména následující právní předpisy:

(Pozn.: není zaručeno, že seznam předpisů je úplný, Obec bude seznam aktualizovat. Odkaz na právní předpis znamená „v platném znění").

Číslo předpisu	Název předpisu
č.128/2000 Sb.	Zákon o obcích (obecní zřízení)
č. 129/2000 Sb.	Zákon o krajích (krajské zřízení)
č. 133/2000 Sb.	Zákon o evidenci obyvatel a rodných číslech
č. 553/1991 Sb.	Zákon o obecní policii
č. 273/2008 Sb.	Zákon o Policii České republiky
č. 141/1961 Sb.	Trestní řád
č. 40/2009 Sb.	Trestní zákoník
č. 328/1999 Sb.	Zákon o občanských průkazech
č. 329/1999 Sb.	Zákon o cestovních dokladech
č. 551/1991 Sb.	Zákon o Všeobecné zdravotní pojišťovně ČR
č. 48/1997 Sb.	Zákon o veřejném zdravotním pojištění
č. 552/1991 Sb.	Zákon o státní kontrole
č. 500/2004 Sb.	Správní řád
č. 262/2006 Sb.	Zákoník práce
č. 106/1999 Sb.	Zákon o svobodném přístupu k informacím, v platném znění
č. 592/1992 Sb.	Zákon o pojistném na všeobecné zdravotní pojištění
č. 634/1992 Sb.	Zákon o ochraně spotřebitele
č. 89/1995 Sb.	Zákon o státní statistické službě
č. 582/1991 Sb.	Zákon o organizaci a provádění sociálního zabezpečení

Obec jako provozovatel, má podle GDPR postavení „**správce**", který zpracovává osobní údaje dotčených osob a odpovídá za toto zpracování. Zpracování osobních údajů je prováděno především pro následující účely:

- uzavírání a provádění smluvních vztahů s jinými subjekty (fyzickými nebo právnickými osobami),
- ochrana a domáhání se práv vůči dalším osobám (občanům, klientům, zaměstnancům apod.),
- zdokumentování činnosti Obce,
- poskytování údajů jiným veřejným orgánům či oprávněným institucím,
- vedení personální a mzdové agendy a evidence zaměstnanců Obce.

Obec jako provozovatel systémů a správce údajů dále zpracovává osobní údaje svých zaměstnanců především pro účely stanovené Zákoníkem práce a ostatními výše uvedenými právními předpisy v oblasti pracovněprávní, daňové oblasti a v oblasti zdravotního a sociálního zabezpečení.

Předmětem činnosti Obce není provádění přímého marketingu, shromážděné a zpracovávané osobní údaje tedy neposkytuje, nezpřístupňuje a nezveřejňuje pro tyto účely.

Jiný účel zpracování osobních údajů může Obec jako „správce" stanovit v souladu se zákonem a způsobem popsaným v této Směrnici.

4 BEZPEČNOSTNÍ OPATŘENÍ

Ochranná (bezpečnostní) opatření jsou praktiky, procedury a mechanismy, které mohou pomoci chránit před hrozbou, snížit zranitelnost, omezit vliv nechtěné události, odhalit nechtěnou událost a umožnit zotavení nebo odškodnění. Přijetím bezpečnostních opatření Obec:

- **neoprávněným osobám** znemožňuje jakýkoliv nedovolený přístup k osobním údajům, manipulaci s technickými zařízeními, určenými pro zpracování osobních údajů a manipulaci s nosiči osobních údajů,
- **oprávněným osobám** zajistí přístup k osobním údajům v rozsahu nezbytném pro plnění jejich pracovních či jiných povinností.

Dělení opatření:

- **technická** – opatření na snížení bezpečnostních rizik pomocí prostředků fyzické a technologické povahy,
- **organizační** (resp. procesní) - opatření na snížení bezpečnostních rizik pomocí změn procesů a úpravou vnitřních pravidel a dokumentace.

Dosažení efektivní bezpečnosti obvykle vyžaduje kombinaci různých bezpečnostních opatření.

Specifikace opatření je soustředěna zejména na následující obsah:

Úkolem technických zabezpečovacích prostředků (např. poplachových systémů na hlášení narušení, systémů průmyslové televize, systémů kontroly vstupů do objektů a systémů sloužících k elektronickému prokazování totožnosti a oprávněnosti osob, systémů na evidenci docházky a systémů elektronické požární signalizace, tísňové systémy, zařízení pro detekci látek a předmětů) je zejména detekovat, vyhodnocovat a zaznamenávat informace z prostředí chráněného objektu o vstupu, přítomnosti, zásazích a pohybu osob, zařízení, věcí nebo dopravních prostředků v chráněných objektech.

Do prostorů Obce mohou neomezeně vstupovatzaměstnanci Obce, vybavení čipem/klíčem (pokud je tento systém zaveden). Pokud má Obecní úřad zaveden docházkový systém, pak každý zaměstnanec je povinen uvést čas příchodu a odchodu do Knihy docházky (vedené v jakékoli podobě, vč. elektronické).

O předání a převzetí klíčů nebo čipu s definovaným oprávněním, je proveden zápis, podepsaný předávajícím a přebírajícím (viz dokument Oprávnění přístupů zaměstnance).

Zaměstnanci nesou plnou zodpovědnost za svěřené klíče/čipy a tyto nesmí v žádném případě předat nebo svěřit jiné osobě (ani zaměstnanci Obce). Pokud se tak stane, vyvodí vedení i vůči tomuto zaměstnanci důsledky.

V případě, že některý ze zaměstnanců ztratí čip nebo mu je odcizen, okamžitě o této skutečnosti informuje starostu a pověřence pro ochranu OÚ.Starosta/ pověřenec zajistí okamžitou blokaci čipu a nahlásí událost jako bezpečnostní incident (viz dokument Bezpečnostní incidenty).

b) Zabezpečení kanceláří, místností a prostředků: vchodové dveřev jednotlivých kancelářích, v archívu jsou trvale uzavřeny v mimo pracovní dobu.
V mimopracovní době jsou trvale zavřena všechna okna, nacházející se v kancelářích.Za zajištění (viz výše) zodpovídá zaměstnanec, který poslední opouští kancelář. Zároveň je tento pracovník povinen **při odchodu zkontrolovat, zda prostory opustili všichni návštěvníci.**

c) Zabezpečení osobních údajů v papírové a elektronické podobě: s osobnímiúdaji a informacemi nakládají zaměstnanci Obce tak, jak stanovuje tato Směrnice a další závazné dokumenty nebo směrnice (viz Pracovní smlouva).

Osobní údaje Obec vhodným způsobem chrání. Nikdo, ani členové vedení, nesmí v žádné podobě (elektronické, papírové, popř. jiné) vynášet z prostoru Obce osobní údaje občanů, zaměstnanců a partnerů. Jedinou výjimkou je transport informací na sekundární úložiště v případě jejich ohrožení.

Za zpracování osobních údajů, za jejich zabezpečení, tedy i uchovávání a likvidaci, jsou zodpovědní všichni zaměstnanci. Zaměstnanci jsou při zpracování osobních údajů povinni je zabezpečit tak, aby nedošlo k jejich zneužití, dodržují **„zásadu prázdného stolu a prázdné obrazovky monitoru"**. Veškeré pracovní, neevidované informace a dokumenty, včetně osobních poznámek zaměstnanců, musí být neprodleně skartovány.

Zaměstnanci mají povinnost zabezpečit osobní údaje v papírové i elektronické podobě tak, aby do nich nemohla nahlížet neoprávněná osoba – občan, návštěva apod.

- Zabezpečení osobních údajů v papírové podobě