Bezpečností politiky a pravidla

(interní dokument)

pro Subjekt:

Apartmány Šnek s.r.o. IČO: 05705932, DIČ: CZ05705932

a tyto provozovny:

Apartmány Šnek Benecko 107 51237

Výše uvedený Subjekt určuje následující bezpečnostní politiky a zásady:

1. Úvodní ustanovení (základní politika)

Subjekt získává a zpracovává informací v elektronické a listinné formě, a to pouze za účelem plnění legislativní povinností a v rozsahu určeném příslušnými zákony.

Subjekt zajišťuje potřebnou důvěrnost, dostupnost, integritu a spolehlivost obsahu informací, které získává a zpracovává způsobem, který je uveden v dalších částech tohoto dokumentu.

Subjekt si je vědom, že nedodržení bezpečnostních požadavků může mít nepříznivé dopady na „subjekty osobních údajů“, tj. zákazníky, resp. hosty nebo může způsobit porušení platné legislativy. Proto Subjekt přijímá závazek k dodržování všech bezpečnostních pravidel a opatření stanovených související legislativou, tímto dokumentem, ostatními vnitřními předpisy a smluvními podmínkami.

1.1. Hlavní bezpečnostní cíle

1. Zajistit přiměřenou bezpečnost informací získaných od hostů a smluvních partnerů, tj. zachovat jejich důvěrnost, zajistit požadovanou dostupnost, integritu a spolehlivost obsahu informací v celém procesu jejich zpracování.
2. Splnit legislativní požadavky na ochranu informací, zejména: nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen GDPR), Zákon o ochraně osobních údajů 101/2000 Sb., Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky, Zákon č. 40/1964 Sb. Občanský zákoník, Zákon č. 513/1991 Sb. Obchodní zákoník a Zákon o účetnictví č. 563/1991 Sb.
3. Splnit požadavky na ochranu informací dodavatelů a smluvních stran.

2. Základní popis informačního systému

Subjekt vede a zpracovává následující agendy, které obsahují dokumenty v listinné i elektronické formě.

3.1. Agendy

Seznam agend:

1. Účetní agenda
   - faktury došlé
   - faktury vydané
   - pokladní doklady
   - účetní kniha
   - evidence majetku
   - hlášení DPH
   - účetní uzávěrky a výsledovky,
   - výkazy pro přiznání k dani a výkazy pro pojišťovny
   - smlouvy s dodavateli a obchodními partnery
2. Agenda hostů
   - kniha ubytování hostů
   - kniha ubytování cizinců
   - objednávky a rezervace
   - smlouvy s hosty
   - vouchery
3. Interní dokumenty
   - ostatní smlouvy
   - interní předpisy
   - interní záznamy
   - bezpečnostní a systémová dokumentace

Agendy jsou vedeny v listinné i elektronické formě.

3.2. Klasifikace informací

Agendy a dokumenty mohou obsahovat následující kategorie údajů:

A. Osobní údaje
B. Interní údaje
C. Ostatní údaje

Subjekt nezískává a nezpracovává žádné informace zvláštní kategorie osobních údajů.

Následující tabulka obsahuje seznam pouze těch dokumentů, které mohou obsahovat osobní údaje. Dále obsahuje určení zákonnosti, účelu zpracování a povolený způsob umístění a povolenou dobu uchování.

Seznam agend a dokumentů obsahující osobní údaje				Místo zpracování				Doba uchování (roky)
Agenda	Dokument	Zákonnost	Účel zpracování údajů	Listina	Počítač	Cloud	Paměťové médium	
Účetní agenda	faktury došlé	563/1991 Sb.	Účetní evidence	x	x	x		10
	faktury vydané	563/1991 Sb.	Účetní evidence	x	x	x		10
	pokladní doklady	563/1991 Sb.	Účetní evidence	x	x	x		
	smlouvy	326/1999 Sb.	Zájem Subjektu i zákazníka	x	x	x		
Agenda hostů	kniha ubytování hostů	326/1999 Sb.	Poplatky obci	x	x			10
	kniha ubytování cizinců	326/1999 Sb.	Cizinecká policie, popl. obci	x	x			10
	objednávky a rezervace	40/1964 Sb.	Zájem Subjektu i zákazníka	x	x	x		
	smlouvy s hosty	40/1964 Sb.	Zájem Subjektu i zákazníka	x	x			
	vouchery	40/1964 Sb.	Zájem Subjektu i zákazníka	x	x	x		
Agenda								

3.3. Rozsah údajů

Rozsah údajů zapisovaných do domovní knihy je ustanovením souladu § 101 zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky vymezen takto:
jméno a příjmení ubytovaného cizince, den, měsíc a rok narození, státní občanství, číslo cestovního dokladu, počátek a konec ubytování.

Rozsah údajů zapisovaných do domovní knihy je v souladu se zákonem č. 565/1990 Sb., o místních poplatcích vymezen takto:

jméno a příjmení, adresa bydliště či zaměstnavatele, číslo občanského průkazu nebo cestovního dokladu, údaje o **datu zahájení a ukončení pobytu**.

Rozsah údajů **pro potřeby účetní evidence, tj. účetní doklady je v souladu se** zákonem č. 563/1991 Sb. o účetnictví stanoven takto:

Název firmy nebo jméno a příjmení fyzické osoby, IČO, DIČ, adresa sídla firmy nebo fyzické osoby, ostatní účetní záznamy, které jsou povinnou náležitostí účetního nebo daňového dokladu.

Pro splnění požadavku transparentnosti jsou tyto údaje zveřejněny na adrese www.snekin.cz v sekci Ochrana osobních údajů.

3.4. Topologie informačního systému

1. PC Mac
2. Bezdrátová síť WIFI
3. Počítač je umístěn v kanceláři subjektu bez přístupu veřejnosti i hostů,
4. Multifunkční zařízení – tiskárna / scaner,
5. Mobilní data – hotspot

5.1. Operační systémy a bezpečnostní SW

1. iOS Apple
2. Aktivní firewal operačního systému
3. Antivirová ochrana operačního systému, pravidelní aktualizace

3.1. Aplikační SW

4. MS Office 365

4.1. Ostatní úložiště informací a způsoby zpracování informací

1. Kancelář provozovny
2. Cloud Google disk

3. Personální bezpečnost (politika řízení lidských zdrojů)

Subjekt deklaruje plnění základních požadavků na informační systém z hlediska personální bezpečnosti vycházející ze zákona č. 412/2005 Sb. a §§ 16 až 19 a vyhlášky č. 523/2005 Sb.

Subjekt nemá žádné zaměstnance. Některé služby mohou být zajištěny smlouvou o dílo na základě smluvního vztahu. Smluvní osoby nemají žádný přístup k agendám a dokumentům subjektu a neprovádějí zpracování informací pro subjekt.

Oprávnění přístupu ke všem agendám má pouze subjekt údajů a spolupracující osoba dle Zákona o dani z příjmů fyzických osob. Touto spolupracující osobou je manželka Subjektu, s níž existuje Smlouva o zpracování osobních údajů.

Za implementaci personální bezpečnostní politiky je odpovědný Subjekt

4. Přístup třetích stran (politika řízení přístupu cizích subjektů)

Poskytovatel připojení internetu O2

Poskytovatel webhostingu www.wpj.cz Firma: WPJ Vrchlabí

Obecní úřad: příjemce údajů

Vzdálený přístup třetích stran je vyloučen.

Kromě poskytovatele účetního informačního systémů všichni ostatní dodavatele neprovádějí zpracování osobních údajů ve smyslu definice GDPR.

Internet pro zákazníky je zprostředkován prostřednictvím interní sítě WIFI, která je oddělena od vnitřní sítě, resp. od aplikací pro zpracování údajů a od systémového bezpečnostního software.

5. Počítačová bezpečnost (politika řízení provozu)

Subjekt deklaruje naplnění minimálních požadavků počítačové bezpečnosti podle §§ 7 a 8 vyhlášky č. 523/2005 Sb., požadavků na ochranu proti kompromitujícímu vyzařování podle § 14 vyhlášky č. 523/2005 Sb., požadavků na bezpečnost při instalaci informačního systému podle § 22 vyhlášky č. 523/2005 Sb. a požadavků na bezpečnost provozovaného informačního systému podle § 23 vyhlášky č. 523/2005 Sb.

V rámci požadavků počítačové bezpečnosti Subjekt deklaruje zejména zajištění:

1. jednoznačné identifikace a autentizace,
2. používání silných hesel,
3. volitelného řízení přístupu k prvkům informačního systému,
4. prokazatelnosti, tj. nepřetržitého zaznamenávání auditních záznamů,

5. ošetření paměťových zařízení před jejich dalším použitím,
6. bezpečnosti vstupně výstupních portů (zejména výměnné nosiče informací),
7. naplnění požadavků komunikační bezpečnosti podle §9 a 9a vyhlášky č. 523/2005 Sb.,
8. ochrany před škodlivým kódem (zejména antivirová ochrana),

Zásady rozšiřování informačního systému:

Každé rozšíření informačního systému musí být zabezpečeno minimálně stejným způsobem, dle stejných zásad a ve stejném rozsahu, jako již implementované části informačního systému.

6. Kryptografická ochrana (politika šifrování)

1. Přenos informací na počítačových médii není povolen. Stejně tak není dovoleno žádné posílání dokumentů obsahující osobní údaje prostřednictvím veřejných sítí včetně e-mail korespondence.
2. Veškeré údaje, které jsou zadávány na portály (cizinecká policie) jsou zajištěny šifrovaným protokolem https. Přístup je zajištěn pomocí autentizace oprávněných uživatelů.

7. Bezpečnost mobilních zařízení (politika mobilních zařízení)

Subjekt neukládá žádné informace o zákaznících do mobilních zařízení, ani neumožňuje on-line připojení jakýchkoliv mobilních zařízení do vnitřní sítě. Subjekt neposkytuje třetím stranám vzdálený přístup.

8. Fyzická bezpečnost

Subjekt používá fyzická zařízení a technologie, které informace ukládají, zpracovávají a zobrazují.

Subjekt deklaruje soulad s požadavky vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Přeprava dokumentů v listinné formě „subjektu osobních údajů“ (zákazník) je zajištěna osobním předáním ze strany Subjektu, nebo jím pověřenou osobou.

Přeprava dokumentů v listinné formě „příjemci údajů“ (Obec Benecko) je zajištěna osobním předáním ze strany Subjektu nebo jím pověřenou osobou.

9. Administrativní bezpečnost (politika řízení informačních aktiv)

Subjekt deklaruje naplnění požadavků administrativní bezpečnosti tím, že definoval agendy a dokumenty, které používá pouze pro splnění účelu legislativních požadavků a k zajištění předmětu své činnosti v nezbytně nutném rozsahu.

Subjekt definoval klasifikaci informací zejména ve vztahu k požadavkům Nařízení EU k ochraně osobních údajů 2016/679 (GDPR). Subjekt určil zákonnost zpracování, kategorie zpracovávaných údajů, účel a rozsah zpracování.

K dokumentům v elektronické i listinné formě má přístup pouze Subjekt nebo jím pověřená osoba, zpravidla manželka Subjektu, příjemce údajů (Obec Benecko, úřady státní správy) nebo sám subjekt osobních údajů (zákazník/host).

Subjekt deklaruje minimální rozsah přepravy dokumentů obsahujících osobní údaje. Hosté nemají přístup k celé knize ubytování, ale vždy vyplňují pouze formuláře pro svoji skupinu nebo apartmán.

Kniha ubytování je uložena v trezoru v kanceláři Subjektu s vyloučením přístupu veřejnosti i hostů. Přeprava knihy k příjemci údajů je prováděna osobním předáním knihy. V elektronické formě je kniha ubytování umístěna pouze na jednom počítači s přístupem pouze Subjektu nebo jím pověřené osoby.

10. Analýza rizik, přezkoumání systému

Subjekt pravidelně identifikuje a vyhodnocuje bezpečnostní rizika, zejména sleduje aktuální hrozby na cscert.cz.

Subjekt přijímá opatření na eliminaci rizik.

Implementovaná bezpečnostní opatření k eliminaci rizik:

- uložení knihy ubytování v trezoru v kanceláři provozovny č. 2 s vyloučením přístupu veřejnosti i hostů,
- minimalizace přepravy dokumentů s osobními údaji v listinné formě,
- vyloučení přepravy dokumentů s osobními údaji v elektronické formě,
- implementace standardních způsobů kybernetické ochrany počítače ve kterém jsou uloženy chráněné agendy (antivirová ochrana, firewall, zálohování, využití bezpečných úložišť typu CLOUD,
- využívání zabezpečených kancelářských aplikaci s možností šifrování obsahu Office 365,

Vzhledem k tomu že:

- jsou splněny požadavky GDPR na zákonnost, účel a rozsah zpracování všech agend obsahující osobní údaje,
- jsou implementována přiměřená bezpečnostním opatření k zajištění bezpečnosti podpůrných aktiv,
- rozsah zpracování osobních údajů je velmi malý, tj. možný dopad na subjekt osobních údajů je nízký,

Subjekt údajů vyhodnotil všechna zbytková rizika, související s bezpečnosti informací obsahující osobní údaje, jako nízká.

Subjekt pravidelně provádí přezkoumání systému a na základě zjištění plánuje bezpečnostní požadavky a zajišťuje potřebné zdroje.