INTERNÍ PŘEDPIS
PRO OCHRANU OSOBNÍCH ÚDAJŮ

podle Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

ve společnosti

SYRMAX, s.r.o., Žitná 5/1670, 110 00 Praha 1, IČ 26116936, DIČ CZ26116936,
Zapsaná v OR u MOS Praha, oddíl C, vložka 71563

Verze	Datum platnosti	Připravil	Schválil
1.0	25.5.2018	Raissa Gbaguidi	Cesare Francorsi

1. ÚVODNÍ USTANOVENÍ

Tento interní předpis upravuje zpracování osobních údajů k zajištění ochrany osobních údajů v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („GDPR“).
Cílem tohoto interního předpisu je zajistit dodržování povinností vyplývajících z GDPR ve společnosti a umožnit subjektům údajů výkon jejich práv.

2. VÝKLAD POJMŮ

Pro účely tohoto interního předpisu se rozumí:

1. „**osobními údaji**“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tj. osobě, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. 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);
2. „**zvláštními kategoriemi osobních údajů**“ osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace

Vypracováno pro interní potřeby členů AHR ČR
ASOCIACE HOTELŮ A RESTAURACÍ ČESKÉ REPUBLIKY

fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

3. „**zpracováním**“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
4. „**omezením zpracování**“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
5. „**správcem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
6. „**zpracovatelem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
7. „**příjemcem**“ 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;
8. „**třetí stranou**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;
9. „**souhlasem**“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
10. „**porušením zabezpečení osobních údajů**“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
11. „**dozorovým úřadem**“ Úřad pro ochranu osobních údajů České republiky
12. „**likvidací**“ osobních údajů se rozumí fyzické zničení jejich nosiče nebo jejich vymazání

SOUVISEJÍCÍ PŘEDPISY A DOKUMENTY

2.1. PRÁVNÍ PŘEDPISY

- Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
- Zákon č. 326/1999 Sb. o pobytu cizinců na území ČR, ve znění pozdějších předpisů
- Zákon č. 565/1990 Sb., o místních poplatcích, ve znění pozdějších předpisů

- Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů
- Zákon č. 586/1992 Sb., o daních z příjmu, ve znění pozdějších předpisů
- Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů
- Zákon č. 143/1997 Sb., o platu a odměně za pracovní pohotovost, ve znění pozdějších předpisů
- Zákon č. 100/1998 Sb., o sociálním zabezpečení, ve znění pozdějších předpisů
- Zákon č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů

3.2 Interní předpisy

1.Pravidla práce s rezervacemi
2.Pravidla pro práci na recepci
3.Pravidla pro práci s platebními kartami
4.Pravidla pro šifrování údajů od dodavatelů SW
5.Pravidla pro archivaci a skartaci
6.Ubytovací řád

3. Role a odpovědnosti

3.1. Zaměstnanci

Každý zaměstnanec odpovídá za to, že zpracování osobních údajů provádí v souladu s právními předpisy a tímto interním předpisem a dalšími předpisy a dokumenty společnosti.
Každý zaměstnanec je povinný zachovávat mlčenlivost o osobních údajích a opatřeních přijatých k jejich ochraně, o nichž se v souvislosti s výkonem svého zaměstnání dozvěděl, a to i po skončení pracovního poměru. Pokud poruší povinnost mlčenlivosti, bude to zaměstnavatel považovat za porušení pracovní kázně zvlášť hrubým způsobem a může se zaměstnancem okamžitě rozvázat pracovní poměr podle § 55 odst. 1 písm. b) zákoníku práce.

4. Zásady zpracování osobních údajů

4.1. Obecné zásady zpracování osobních údajů

Při zpracování osobních údajů ve společnosti je nezbytné dodržovat následující zásady:

a) ve vztahu k subjektu údajů musí být osobní údaje zpracovávány korektně, zákonným a transparentním způsobem („**zákonnost, korektnost a transparentnost**“);
b) osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný („**účelové omezení**“);
c) zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány („**minimalizace údajů**“);

d) osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („**přesnost**“);
e) osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány („**omezení uložení**“);
f) osobní údaje musí být 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**“);

5. TECHNICKO-ORGANIZAČNÍ OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

Systém ochrany osobních údajů je tvořen komplexem organizačních a technických opatření, která jsou ve společnosti realizována za účelem zabezpečení ochrany a bezpečnosti osobních údajů.

5.1. BEZPEČNOSTNÍ OPATŘENÍ

Řízení rizik

Revize vyhodnocení rizik je ve společnosti prováděna pravidelně 1 krát ročně. Ad hoc revize rizik je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů nebo v případě narušení zabezpečení ochrany osobních údajů. Za provedení revize odpovídá odpovědná osoba.

Vyhodnocení rizik uvažuje následující:
a) Riziko vůči právům a svobodám subjektů údajů z následujících pohledů
1. Porušení principů přiměřenosti a nezbytnosti zpracování
2. Porušení práv subjektů údajů
3. Neoprávněný přístup k osobním údajům
4. Neoprávněná změna osobních údajů
5. Nedostupnost nebo výmaz osobních údajů

b) Možný dopad v případě realizace rizik v písm. a). (například zpracování osobních údajů bez právního titulu může vést k zasílání nevyžádaných obchodních sdělení nebo neschopnosti zajistit výkon práva subjektu údajů a následnému způsobení hmotné či nehmotné újmy, neoprávněný přístup k citlivým osobním údajům může vést k odcizení identity apod.).

c) Hodnocení závažnosti dopadu: Na základě definice možných dopadů v bodě b) je určena jedna z následujících kategorií.
1. Zanedbatelné: Subjekty údajů nebudou dotčeny, nebo budou dotčeny minimálně bez jakýchkoliv větších problémů (např. opětovné zadávání informací do systému, obtěžování při opětovném marketingovém sdělení)

2. Omezené: Subjekty údajů se mohou setkat s nepříjemnostmi, které budou schopny relativně snadno vyřešit (dodatečné náklady, popření přístupu k obchodním službám, strach, nedostatek porozumění, stres atd.).
3. Významné: Událost může mít významný důsledek pro subjekty údajů. Tyto důsledky by subjekty měly být schopné překonat, ačkoliv s vážnými obtížemi (např. zneužití finančních prostředků, škody na majetku, ztráta zaměstnaní, zhoršení zdravotního stavu atd.)
4. Vysoké: Událost může mít vysoké nebo nezvratné důsledky pro subjekty údajů, které nemusí být možné překonat (např. finanční potíže, značný dluh, pracovní neschopnost, dlouhodobé fyzické nebo psychické nemoci, smrt atd.)

d) Hodnocení pravděpodobnosti výskytu události, která může mít negativní vliv na subjekty údajů. Tato metodika uvažuje následující kategorie:
1. Zanedbatelné: Ve společnosti ani v odvětví se událost ještě nevyskytla, její výskyt však není vyloučený.
2. Omezené: Ve společnosti se událost v minulosti ještě nevyskytla, její výskyt však byl již zaznamenán v rámci odvětví.
3. Významné: Ve společnosti se událost v minulosti již vyskytla.
4. Vysoké: Ve společnosti se událost již vyskytla opakovaně.

e) Zavedená a plánovaná ochranná resp. nápravná opatření

Fyzická bezpečnost

- *Pro kontrolu fyzického přístupu do prostor společnosti je využíváno recepce. Vstup je umožněn pouze oprávněným osobám.*
- *Fyzické bariéry jsou tam, kde je to použitelné, postaveny tak, aby chránily před neoprávněným vstupem a kontaminací.*
- *Požární dveře jsou v definovaném bezpečnostním perimetru opatřeny elektronickým zabezpečovacím systémem a jsou monitorovány.*
- *Vnější dveře a dosažitelná okna jsou chráněny vhodným detekčním systémem, který odpovídá místním, národním a mezinárodním normám a je pravidelně testován.*
- *Zařízení pro zpracování informací spravované organizací jsou fyzicky oddělena od prostředků neoprávněných osob.*
- *Není dovoleno nechávat osobní údaje volně k dispozici bez dohledu. Platí, že písemnosti a jiné nosiče osobních údajů je dovoleno uchovávat samostatné pouze v uzamykatelných místnostech, případně pouze v uzamykatelných skříních.*
- *Přístup do kanceláří nebo archivů, kde jsou tyto osobní údaje uloženy, je umožněn pouze oprávněným zaměstnancům společnosti a to pomocí fyzického klíče.*
- *Prostory společnosti, ve kterých jsou uloženy osobní údaje, jsou pod 24 hodinovým kamerovým dohledem. Zpracování formou kamerového systému je upraveno v samostatném interním předpise .*
- *Fyzický přístup do serverovny je umožněn pouze pracovníkům IT.*
- *Je vyžadováno dodržování zásady prázdného stolu a zamknuté obrazovky.*

Narušení zabezpečení osobních údajů

V případě zjištění porušení zabezpečení osobních údajů je nezbytné:

1. *Oznámit zjištění odpovědné osobě*
2. *Zamezit dalšímu úniku – fyzickým zamčením dokumentů nebo v případě elektronické formy zamezením přístupu nebo vypnutím IT systémů*
3. *Případ narušení zabezpečení posoudit a zdokumentovat (co se stalo, jaké a čí osobní údaje unikly, možné následky, popis přijatých opatření s cílem vyřešit daný případ, identifikace rizika/vysokého rizika)*
4. *Ohlásit porušení zabezpečení dozorovému úřadu bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm společnost dozvěděla, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob*
5. *Oznámit porušení zabezpečení bez zbytečného odkladu subjektu údajů pokud je pravděpodobné, že daný případ bude mít za následek vysoké riziko pro práva a svobody fyzických osob*

Kontaktní místo pro oznámení zjištění porušení zabezpečení:	*Raissa Gbaguidi* *raissa@yourpraguehotels.com*

Kontrolní činnost

Osoby odpovědné za jednotlivé oblasti dle katalogu zpracování osobních údajů (viz příloha), zajistí kontrolu plnění povinností vyplývajících z tohoto interního předpisu. Kontroly jsou prováděny v následujícím rozsahu:

a) *1 krát ročně důkladná kontrola celé společnosti odpovědnou osobou*
b) *1 krát měsíčně namátková kontrola vybraného informačního systému nebo úseku odpovědnou osobou*
c) *Každodenně kontrola fyzické ochrany rizikových míst odpovědnou osobou*
d) *Kontrola po změně a následném školení ke změnám zákonů nebo interních předpisů, včetně tohoto interního předpisu*
e) *Mimořádná kontrola po řešení narušení zabezpečení osobních údajů*

O pravidelných kontrolách je proveden záznam a ten je uložen. V případě nálezů kontroly probíhá konzultace, případně ad hoc proškolení.

Školení zaměstnanců

Proškolování zaměstnanců probíhá formou školení na pracovišti, zaměřeného na informační bezpečnost a ochranu osobních údajů a to jak při nástupu, tak pravidelně alespoň 1 krát ročně. Evidence o absolvování školení je zpracovávána personálním oddělením společnosti. Za proškolení zaměstnanců odpovídá odpovědná osoba.

5.2. Ostatní opatření

Pravidelná revize a aktualizace interních předpisů

Všechny interní předpisy společnosti, včetně těch, týkajících se ochrany osobních údajů jsou revidovány pravidelně 1 krát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů nebo v případě narušení zabezpečení ochrany osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá odpovědná osoba.

Vedení a aktualizace katalogu zpracování

Katalog zpracování v příloze tohoto dokumentu je součástí pravidelné revize a aktualizace interních předpisů. Revize kompletnosti a přesnosti katalogu zpracování je prováděna pravidelně 1 krát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá odpovědná osoba.

Zpracovatelské vztahy

Výběr zpracovatelů schvaluje odpovědná osoba. Při výběru zpracovatelů hodnotí zejména následující faktory:

- *Schopnost dodavatele uzavřít a dodržovat povinnosti stanovené zpracovatelskou smlouvou*
- *Dostatečné zabezpečení osobních údajů*
- *Dobrá pověst dodavatele v rámci ochrany osobních údajů*
- *Relevantní certifikace ochrany osobních údajů nebo ochrany informací obecně (např. ISO 27k apod.)*
- *Další relevantní faktory ve vztahu ke konkrétnímu účelu zpracování*

Řízení projektů a změn

V případě významnějších změn ve společnosti s dopadem na ochranu osobních údajů (např. nový IT systém, nový účel zpracování, včetně nové služby nebo produktu, apod.) je do těchto aktivit zapojena odpovědná osoba, která identifikuje případná rizika pro ochranu osobních údajů a pomůže navrhnout adekvátní opatření ke snížení těchto rizik. V případě potřeby provede revizi a aktualizaci tohoto interního předpisu, včetně analýzy rizik nebo aktualizace katalogu zpracování, případně dalších relevantních interních předpisů.

Předávání osobních údajů do třetích zemí

Při předávání osobních údajů do třetích zemí postupuje společnost v souladu s kapitolou V. GDPR.
V rámci činnosti společnosti dochází k přenosu dat do třetích zemí na základě smluvního vztahu mezi prodejcem a spotřebitelem.

6. VÝKON PRÁV SUBJEKTŮ ÚDAJŮ

POSKYTOVÁNÍ INFORMACÍ

Společnost poskytuje subjektům údajů informace v souladu s článkem 13 a 14 GDPR a to v požadovaném rozsahu, čímž zajišťuje transparentnost zpracování.
Informace o zpracování osobních údajů hostů je součástí registrační karty, webových stránek a ubytovacího řádu.

PRÁVO SUBJEKTŮ ÚDAJŮ NA PŘÍSTUP K OSOBNÍM ÚDAJŮM

V případě, že o to subjekt údajů požádá, společnost poskytne subjektu údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, umožní subjektům údajů získat přístup k těmto osobním údajům a k informacím způsobem a v rozsahu dle článku 15 GDPR.

PRÁVO NA OPRAVU

V případě, že o to subjekt údajů požádá, případně se o nepřesných osobních údajích dozví společnost jinak, opraví bez zbytečného odkladu nepřesné osobní údaje. V případě, kdy si to účel zpracování vyžaduje, zajistí společnost doplnění neúplných osobních údajů dle článku 16 GDPR.

PRÁVO NA VÝMAZ

V případě, že je dán jeden z následujících důvodů, zajistí společnost na základě uplatnění práva subjektem údajů bez zbytečného odkladu výmaz osobních údajů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;
b) subjekt údajů odvolá souhlas, na jehož základě byly osobních údaje zpracovávány, a neexistuje žádný další právní důvod pro zpracování;
c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být vymazány ke splnění právní povinnosti, která se na společnost vztahuje;
f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 GDPR.

PRÁVO NA OMEZENÍ ZPRACOVÁNÍ

V případě, že je dán jeden z následujících důvodů, zajistí společnost omezení zpracování osobních údajů:

a) subjekt údajů popírá přesnost osobních údajů;
b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
c) společnost již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
d) subjekt údajů vznesl námitku proti zpracování.

PRÁVO NA PŘENOSITELNOST ÚDAJŮ

V případě, že o to subjekt údajů požádá a zároveň je zpracování založeno na souhlasu nebo smlouvě, a zároveň se zpracování provádí automatizovaně, umožní společnost subjektu údajů výkon práva na přenositelnost. Osobní údaje, které subjekt údajů společnosti poskytl a které se ho týkají, poskytne společnost ve strukturovaném, běžně používaném a strojově čitelném formátu. Součástí tohoto práva je zajištění možnosti přenesení předmětných osobních údajů k jinému správci dle požadavku subjektu údajů.

7. ARCHIVACE A LIKVIDACE OSOBNÍCH ÚDAJŮ

7.1. ARCHIVACE

Archív je provozován samotným správcem. Rozsah údajů k archivaci a archivační doba vyplývá z katalogu zpracování osobních údajů (příloha č. 1 tohoto dokumentu). Přístup do archivu mají pracovníci externí firmy, která vede účetnictví a personální agendu a jen osoby v konkrétních pracovních pozicích za předem daným důvodem a pro naplnění některého z účelů předvídaných GDPR

.

Pracovní pozice	***Kategorie osobních údajů***	***Důvod přístupu do archivu***
Manažer hotelu	*Jméno, příjmení, adresa trvalého pobytu, počátek a konec ubytování*	*Podání informace o pobytu klienta na základě žádosti cizinecké policie*

- *Archivace osobních údajů hostů*

  Archivace osobních údajů hostů se řídí mj. § 101 zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky, který ukládá povinnost ubytovateli vést domovní knihu a uchovávat ji po dobu 6 let od posledního zápisu. Podle zákona č. 565/1990 Sb., o místních poplatcích, vede organizace v písemné podobě evidenční knihu, do které zapisuje dobu ubytování, účel pobytu (účel a doba se neeviduje v knize u poplatku z ubytovací kapacity), jméno, příjmení, adresu místa trvalého pobytu nebo místa trvalého bydliště v zahraničí a číslo občanského průkazu nebo cestovního dokladu fyzické osoby, které ubytování poskytl. Zápisy do evidenční knihy jsou vedeny přehledně a srozumitelně a jsou uspořádány chronologicky. Evidenční kniha se uchovává po dobu 6 let od provedení posledního zápisu.

7.2. LIKVIDACE

Společnost provádí likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovávány, případně na základě žádosti subjektu.
Při likvidaci jsou dodržovány zákonné výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.
Likvidace osobních údajů je prováděna certifikovanou externí společností na základě smlouvy o zpracování osobních údajů. O skartaci je vydáno potvrzení.

8. ZÁVĚREČNÁ USTANOVENÍ

- Za dodržování interního předpisu odpovídají všichni zaměstnanci společnosti.
- Zaměstnanci stvrzují svým podpisem, že byli seznámeni s tímto interním předpisem.
- V Praze 23.5.2018