POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**" (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Spółce Przedsiębiorstwo Produkcyjno - Handlowe "Wrzos" Spółka z ograniczoną odpowiedzialnością (dalej jako: **Spółka**) w ramach obiektu hotelowego SPA Bagiński & Chabinka, Ośrodek Wypoczynku i Odnowy Biologicznej, zlokalizowanego w Międzyzdrojach (72-500) przy ul. Gryfa Pomorskiego 74 (zwanego dalej: **Obiektem**).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Administratorem Danych Osobowych (dalej: ADO) jest: Przedsiębiorstwo Produkcyjno - Handlowe "Wrzos" Spółka z ograniczoną odpowiedzialnością z siedzibą w Międzyzdrojach (72-500) ul. Orla, nr 4, lok. E, posiadająca nr: REGON: 811023269, NIP: 8512122911, wpisana do rejestru przedsiębiorców KRS pod nr 0000071011.

2. Polityka zawiera informacje o celu przetwarzania danych osobowych, opis zasad ochrony danych obowiązujących w Spółce – w ramach Obiektu; przy odwołaniu do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

3. Odpowiedzialny za:

a) wdrożenie i utrzymanie niniejszej Polityki - jest Zarząd Spółki (a w ramach Zarządu - Członek Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych);

b) nadzór i monitorowanie przestrzegania Polityki - jest Inspektor Ochrony Danych Osobowych,

4. Do stosowanie niniejszej Polityki zobowiązani są:

a) Spółka;

b) wszyscy członkowie personelu Spółki, w tym w szczególności członkowie personelu zatrudnieni w działach:

- recepcji,

- zarządzania i marketingu,

- SPA,

- gastronomii,

- kadr,

- księgowości.

Ponadto spółka zapewnia zgodność postępowania kontrahentów Obiektu z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

5. Skróty i definicje:

Polityka oznacza niniejszą Politykę ochrony danych osobowych.
RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
Dane wrażliwe oznaczają dane specjalne i dane karne.
Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
Dane dzieci oznaczają dane osób poniżej 16. roku życia.
Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
Podmiot przetwarzający oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).
Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się – przy czym
ADO oznacza Administratora Danych Osobowych.
IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych.
RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
PBI oznacza Politykę Bezpieczeństwa Informacji odzwierciedlającą i opisującą system zarządzania bezpieczeństwem informacji z zakresu danych osobowych;
Umowa hotelowa – umowa przez którą Spółka **zobowiązuje się:**
- oddać Gościowi za umówionym wynagrodzeniem pokój w Obiekcie w oznaczonym terminie w używanie wraz z dostępem do strefy SPA (obejmującym dostęp do basenu, jacuzzi, łaźni i sauny) oraz dostępem do sali fitness;
- oraz spełniać ewentualne dodatkowe – towarzyszące - usługi i świadczenia a także czuwać nad wniesionymi przez gościa rzeczami.

Usługi i świadczenia towarzyszące – dodatkowe usługi i świadczenia przysługujące poza noclegiem Gościowi Obiektu wliczone w cenę oznaczoną w umowie hotelowej bądź płatne za dodatkowym wynagrodzeniem, obejmujące w szczególności usługi SPA, usługi restauracji Obiektu, usługi coctail – baru Obiektu, usługi parkingu zlokalizowanego na terenie Obiektu, usługi wynajęcia rowerów, usługi wynajęcia kijów do nordic walking, usługi wynajęcia leżaków plażowych, parawanów oraz parasoli plażowych, świadczenia zakupu kwiatów, butelki wina, patery owoców.
Usługa SPA – usługa świadczona na terenie Obiektu obejmująca usługi o charakterze fizjoterapeutycznym, kosmetycznym bądź pielęgnacyjnym.

6. Ochrona danych osobowych w Spółce – zasady ogólne

6.1. Filary ochrony danych osobowych w Spółce:

(1) **Legalność** − Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** − Spółka zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa Jednostki** − Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) **Rozliczalność** − Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

6.2. Zasady ochrony danych

Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:

(1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

(2) rzetelnie i uczciwie (rzetelność);

(3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

(4) w konkretnych celach i nie „na zapas” (minimalizacja);

(5) nie więcej niż potrzeba (adekwatność);

(6) z dbałością o prawidłowość danych (prawidłowość);

(7) nie dłużej niż potrzeba (czasowość);

(8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

6.3. System ochrony danych

System ochrony danych osobowych w Spółce składa się z następujących elementów:

1) Inwentaryzacja danych. Spółka dokonuje identyfikacji zasobów danych osobowych w Spółce, w tym:

a) przypadków przetwarzania danych specjalnych w zakresie danych o stanie zdrowia Gości Obiektu (**dane wrażliwe**);

b) przypadków przetwarzania danych osób, których Spółka nie identyfikuje (**dane niezidentyfikowane**/UFO) w szczególności poprzez zastosowanie monitoringu;

c) przypadków przetwarzania danych dzieci;

d) profilowania;

e) współadministrowania danymi.

2) **Rejestr.** Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Spółce (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Spółce.

3) **Podstawy prawne.** Spółka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

   a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

4) **Obsługa praw jednostki.** Spółka spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

   a) **Obowiązki informacyjne.** Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

   b) **Możliwość wykonania żądań.** Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

   c) **Obsługa żądań.** Spółka zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

   d) **Zawiadamianie o naruszeniach.** Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** Spółka posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

   a) zasady zarządzania **adekwatnością** danych;

   b) zasady reglamentacji i zarządzania **dostępem** do danych;

   c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

   a) stosuje Politykę Bezpieczeństwa Informacji;

   b) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii oraz przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie, a także dostosowuje środki ochrony danych do ustalonego ryzyka;

   c) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

7) **Przetwarzający.** Spółka posiada zasady doboru przetwarzających dane na rzecz Spółki, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) ***Privacy by design*.** Spółka zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

7. Inwentaryzacja

6.1. Dane wrażliwe

Spółka identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.2. Profilowanie

Spółka identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.3. Współadministrowanie

Spółka identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

8. Rejestr Czynności Przetwarzania Danych

7.1. RCPD stanowi formę dokumentowania czynności przetwarzania danych (poprzez inwentaryzację czynności przetwarzania danych osobowych), w jaki wykorzystuje dane osobowe w myśl zasady rozliczalności.

9. Podstawy przetwarzania

8.1. Spółka wskazuje, że podstawą przetwarzania danych osobowych klientów - Gości Obiektu są:

- umowy hotelowe (obejmująca świadczenie usługi hotelowej oraz usług towarzyszących);

- umowy allomentu;

zawarte na podstawie art. 353^1 k.c.

8.2. Spółka wskazuje, że podstawą przetwarzania danych osobowych pozostałych klientów niebędących Gośćmi Obiektu są:

- umowy wynajmu sal szkoleniowych;

- umowy świadczenia usług SPA;

- umowy cateringu;

zawarte na podstawie art. 353^1 k.c. bądź 734 k.c.

8.3. Spółka wskazuje również, że może przetwarzać dane wrażliwe klientów korzystających z usług SPA w zakresie danych o stanie zdrowia (w szczególności dane o braku przeciwwskazań zdrowotnych do poszczególnych zabiegów) w celu prawidłowej realizacji usług SPA.

8.4. Spółka dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.5. Spółka wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności.

8.6. Kierownik działu Obiektu prowadzonego w ramach Spółki ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

9.1. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

9.2. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce,

9.3. W celu realizacji praw jednostki Spółka zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Spółkę, zintegrować te dane, wprowadzać do nich zmiany i usuwać,

9.4. Spółka dokumentuje obsługę obowiązków informacyjnych, zgód, zawiadomień i żądań osób.

10. Obowiązki informacyjne

10.1. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

10.2. Spółka informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

10.3. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

10.4. Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (w szczególności poprzez zamieszczenie tabliczki o objęciu obszaru monitoringiem wizyjnym).

10.5. Spółka informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

10.6. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania danych.

10.7. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

11. Żądania osób

11.1. **Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, Spółka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Spółka może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

11.2. **Odmowa**. Spółka informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

11.3. **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, Spółka informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących.

11.4. **Sprostowanie danych**. Spółka dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.

11.5. **Uzupełnienie danych**. Spółka uzupełnia i aktualizuje dane na żądanie osoby. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych.

11.6. **Usunięcie danych.** Na żądanie osoby, Spółka usuwa dane, gdy:

(1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

(2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(4) dane były przetwarzane niezgodnie z prawem,

(5) konieczność usunięcia wynika z obowiązku prawnego,

Spółka określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

11.7. **Ograniczenie przetwarzania.** Spółka dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

(1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

(2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

(3) Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

(4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Spółka przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

11.8. Przenoszenie danych. Na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.

11.9. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

11.10. Sprzeciw przy celach statystycznych. W związku z realizacją celów statystycznych przez Spółkę, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania.

11.11. Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

12. MINIMALIZACJA

Spółka dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

12.1. Minimalizacja zakresu

Spółka weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

Spółka może przetwarzać dane osobowe Gości Obiektu podane dobrowolnie w celach realizacji umowy hotelowej. Powyższe dane osobowe obejmować mogą:
- imię nazwisko,
- adres e-mail lub numer telefonu,
- adres zamieszkania,

- firma i numer NIP (w przypadku, gdy rozliczenie należności względem Spółki następuje na podstawie faktury VAT).
Spółka może przetwarzać również powyższe dane na podstawie zgody Gości Obiektu w celach marketingowych.

Spółka może przetwarzać dane o stanie zdrowia Gości Obiektu korzystających z usług SPA (np. przeciwwskazania do zabiegu na karcie zabiegowej) w celach realizacji powyższych usług.

Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

Spółka przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

12.2. Minimalizacja dostępu

Spółka stosuje ograniczenia dostępu do danych osobowych:
- prawne (w szczególności poprzez zobowiązania do poufności, zakresy upoważnień),
- fizyczne (strefy dostępu, zamykanie pomieszczeń),
- logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

Spółka stosuje kontrolę dostępu fizycznego.
Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa informacji Spółki.

12.3. Minimalizacja czasu

Spółka wdraża mechanizmy kontroli cyklu życia danych osobowych w Spółce, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych Spółki. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

W każdym przypadku dane osobowe Gości Obiektu są usuwane po 10 latach od dnia wymeldowania się z hotelu. Zachowanie 10 – letniego okresu jest konieczne z uwagi na termin przedawnienia roszczeń wynikający z art. 118 k. c.

13. BEZPIECZEŃSTWO

Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Spółkę.

13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

Spółka przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają (w ramach tzw. matrycy ryzyka), spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa, w szczególności może posłużyć się: anonimizacją, pseudonimizacją, szyfrowaniem danych osobowych oraz innymi środkami składającymi się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

13.2. Środki bezpieczeństwa

Spółka stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Spółce.

13.3. Zgłaszanie naruszeń

Spółka stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

14. PRZETWARZAJĄCY

Spółka posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Spółki opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Spółce.

15. PROJEKTOWANIE PRYWATNOŚCI

Spółka zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
W tym celu zasady prowadzenia projektów i inwestycji przez Spółkę odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.