POLITYKA BEZPIECZEŃSTWA
W ZAKRESIE DANYCH OSOBOWYCH
W HOTELU KOSMOWSKI

SPIS TREŚCI

WSTĘP

Informacje ogólne

Firma „KOS ELEKTRO SYSTEM" jest właścicielem Hotelu Kosmowski. Hotel świadczy usługi w zakresie noclegu i usług restauracyjnych, organizacji wesel i imprez rodzinnych, organizacji szkoleń firmowych oraz usług towarzyszących.

Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Hotelu Kosmowski z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych oraz uchylenia dyrektywy95/46/WE (ogólne rozporządzenie o ochronie danych) i Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi.

Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

-Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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/W

Politykę Bezpieczeństwa stosuje się do:

- danych osobowych przetwarzanych w systemie informatycznym,

-wszystkich informacji dotyczących danych gości hotelu,

-wszystkich informacji dotyczących pracowników,

- informacji dotyczących zabezpieczenia danych osobowych, w tym szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,

- rejestru osób dopuszczonych do przetwarzania danych osobowych,

- innych dokumentów zawierających dane osobowe.

Zakres informacji objętych polityką bezpieczeństwa oraz zakres zastosowania

- zbiory danych osobowych w formie papierowej:

Karta meldunkowa, karta parkingowa, rezerwacje w formie papierowej, dokumenty księgowe (faktury, paragony, dokumenty kasowe), umowy z klientami w wersji papierowej, kalendarz imprez.

Powyższe dane znajdują się w niedostępnych dla osób trzecich zamkniętych na klucz szafach w biurze Dyrektora, w recepcji hotelu.

- zbiory danych osobowych w formie elektronicznej:

Program komputerowy PLAZA, korespondencja e:mail z książką adresową.

Administrator może przetwarzać dane osobowe wyłącznie wtedy, gdy istnieje tzw. podstawa przetwarzania danych.

Podstawą przetwarzania danych osobowych jest:
- zgoda osoby, której dane dotyczą
- przetwarzanie danych jest niezbędne do wykonania umowy z osobą, której dane dotyczą lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby,
- przetwarzanie jest niezbędne do wypełniania obowiązku prawnego ciążącego na administratorze,
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.

W przypadku szczególnych kategorii danych osobowych (ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe) podstawy przetwarzania tych danych to:
-wyraźna zgoda osoby, której dane dotyczą,
-przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem.

Monitoring

Administrator danych jest uprawniony do stosowania monitoringu, dla zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę będącego Administratorem Danych na szkodę. Monitoring jest dopuszczalny wewnątrz hotelu jak i na zewnątrz. Administrator danych jest obowiązany do stosowania Polityki Bezpieczeństwa do pozyskanych za pośrednictwem monitoringu danych w szczególności wizerunku osób, w tym minimalizacji danych i retencji danych oraz ochronę tych danych.

Nagrania obrazu Administrator danych przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nieprzekraczający 7 dni od dnia nagrania.
W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin przechowywania nagrań ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
Po upływie okresów, powyższych uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe, podlegają zniszczeniu.

Administrator danych jest zobowiązany do prowadzenia dokumentacji monitoringu zawierającej: (załącznik nr 3)
- wykaz obszarów monitorowanych,
- wykaz środków rejestrujących,
- wykaz sposobu przechowywania zapisu monitoringu i wskazanie środków technicznych zabezpieczających dostęp do zapisów monitoringu,
- wykaz upoważnionych osób posiadających dostęp do monitoringu.

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

Osobami odpowiedzialnymi za ochronę danych osobowych w hotelu są:
- Administrator danych,
- Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora danych osobowych,
- Osoby upoważnione przez Administratora danych do przetwarzania danych osobowych
(załącznik nr 1)

Administratorem danych osobowych jest Kos Elektro System Sp. z o.o. z siedzibą we Wrześni, przy ul. Wrocławska 43, zarejestrowaną pod numerem KRS 0000031844 w Rejestrze Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonym przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, XI Wydział Gospodarczy Krajowego Rejestru Sądowego, posiadającą NIP: 7891565060, REGON: 634213660, kapitał zakładowy 3.3000.000 złotych, reprezentowaną przez: Ryszard Kosmowski – Prezes Zarządu, Sylwia Kosmowska – Wiceprezes Zarządu.
Obowiązkiem Administratora jest zapewnienie zgodności jego i osób, którym powierzył dane do postępowania zgodnie z obowiązującym prawem krajowym i unijnym. Administrator danych wykazuje, że dysponuje odpowiednią podstawą przetwarzania danych.
Obowiązkiem Administratora jest ustalenie, jakie dane osobowe, w jakim charakterze, po co i w jakim środowisku przetwarza, określenie ryzyka naruszenia praw lub wolności osób fizycznych związane z takim przetwarzaniem, dobranie odpowiednich środków zabezpieczenia danych, uwzględniając istniejące możliwości techniczne i własne możliwości finansowe.

Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych jest zobowiązana do ich ochrony w sposób zgodny z przepisami Ustawy o ochronie danych osobowych, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 i Polityki Bezpieczeństwa.
Osoba upoważniona jest zobowiązana do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
(załącznik nr 5). Oryginały upoważnień znajdują się w dziale kadr firmy, do Polityki Bezpieczeństwa dołączono kopie upoważnień.

PRZETWARZANIE DANYCH OSOBOWYCH

Przy gromadzeniu danych Administrator ma obowiązek przekazywać osobie, której dane dotyczą następujące informacje:
- o tożsamości Administratora danych i o jego danych kontaktowych,
- o celach i podstawie przetwarzania danych, a jeżeli przetwarzanie odbywa się nam tej podstawie, ż jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – o tych prawnie uzasadnionych interesach,

- o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- o okresie czasu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie zgody – o prawie do cofnięcia zgody w dowolnym momencie,
- o prawie wniesienia skargi do organu nadzorczego, informacji czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i dokumentów w formie papierowej odbywa się wyłącznie w obszarze przetwarzania danych, pomieszczeniach na terenie hotelu.

Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych, wyłącznie za zgodą Administratora danych.
Wykaz z pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe zawiera załącznik nr 2.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba, że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
Podmiot występujący o udostępnienie danych osobowych powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy będzie ono stanowić naruszenie zasad ochrony danych osobowych.

Udostępnienie danych osobowych może nastąpić jedynie za zgodą Administratora danych lub osoby przez niego upoważnionej.

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby drzwi wejściowe były tak zabezpieczone by otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby. Pracownicy Administratora danych są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe.

W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.

OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawienie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Osoby przetwarzające dane osobowe w formie elektronicznej zobowiązane są do każdorazowego blokowania komputera hasłem i wylosowania się z programu przetwarzającego dane w przypadku każdego, w tym krótkotrwałego opuszczenia miejsca pracy.
Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w sklad obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności, w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach.
Pracownicy zo0bowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy prze nieuprawnionym dostępem.

PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

Każdy użytkownik, przed dopuszczeniem przetwarzania danych osobowych, podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań i obowiązków.
Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym – wymiana sprzętu do nowszej generacji, zmiana oprogramowania – oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.
Za organizację szkoleń odpowiedzialny jest Administrator danych osobowych.

Użytkownik powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.

Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych należą:
- wydzielenie pomieszczeń,
- wyposażenie pomieszczeń w odpowiednie szafy zamykane na klucz,
- zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami,
- szczególne zabezpieczenie centrum przetwarzania danych, komputera poprzez zastosowanie systemu kontroli dostępu – hasła.

Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko użytkownicy.
Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych niż upoważnionych przez Administratora danych, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora danych.

Klucze do pomieszczeń przechowywane są w pomieszczeniu, gdzie przebywają osoby upoważnione przez Administratora danych. Klucze wydawane są wyłącznie osobom do tego upoważnionym.

Dokumenty w formie papierowej należy przechowywać w szafach- zamkniętych na klucz, do których dostęp mają wyłącznie użytkownicy upoważnieni przez Administratora danych.
Użytkownicy upoważnieni przez Administratora danych, odpowiedzialni są za rzetelne prowadzenie dokumentów, ich kompletność oraz ochronę.

OPIS ZDARZEŃ NARUSZAJĄCYH OCHRONĘ DANYCH OSOBOWYCH

Podział zagrożeń:

- zagrożenia losowe zewnętrzne, np. klęski żywiołowe, przerwy w zasilaniu, ich występowanie może prowadzić do utraty integralności danych, ich zniszczeniu i uszkodzeniu infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
- zagrożenia losowe wewnętrzne, np. niezamierzone pomyłki pracowników, administratora, awarie sprzętowe, błędy oprogramowania, może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
- zagrożenia zamierzone, świadome, celowe – najpoważniejsze zagrożenia naruszenia poufności danych. Zazwyczaj ie następuje uszkodzenie infrastruktury technicznej i zakłócenia ciągłości pracy. Zagrożenia możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lun inną nadzwyczajną i niepożądaną modyfikację w systemie,
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,

- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylosowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych).
- praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu.

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych: otwarte szafy, biurka, urządzenia archiwalne i inne, na nośnikach tradycyjnych, tj. na papierze – wydruki, zdjęcia w formie niezabezpieczonej.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Danych.
Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych lub upoważnionej przez nich osoby, osoba powiadamiająca powinna:
- niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
- zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator Danych:
- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,
- wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również\ relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

Administrator Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych, proponuje postępowanie naprawcze, ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń i zarządza termin wznowienia przetwarzania danych.

POSTĘPOWANIE W WYPADKU KLĘSKI ŻYWIOŁOWEJ

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

O zagrożeniu, jego skali i podjętych krokach zaradczych pracownik zobowiązany jest niezwłocznie powiadomić Administratora Danych, w każdy możliwy sposób. W razie niemożności skontaktowania się z nim pracownik zawiadamia osobę wyznaczoną przez Administratora Danych.

Numery telefonów Administratora Danych i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe.

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, zobowiązani są do przerywania pracy – w miarę możliwości przed opuszczeniem tych pomieszczeń do:

- zamknięcia systemu informatycznego,
- zabezpieczenia danych osobowych gromadzonych w kartotekach.

W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych i obecni pracownicy powinni w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.

Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych obecnych przy akcji ratunkowej.

MONITOROWANIE ZABEZPIECZEŃ

Prawo do monitorowania systemu zabezpieczeń posiada Administrator Danych.

W ramach kontroli należy zwracać uwagę na:

- okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
- kontrola ewidencji nośników magnetycznych,
- kontrola właściwej częstotliwości zmiany haseł.

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA OCHRONY DANYCH OSOBOWYCH

Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Hotelu Kosmowski sprawuje Administrator Danych.

Administrator Danych ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych.

Administrator Danych Osobowych w przypadku swojej nieobecności, wyznacza osobę, która go zastępuje.

POSTANOWIENIA KOŃCOWE

Polityka jest dokumentem wewnętrznym i nie może być udostępniana w żadnej formie.

Administrator Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z Polityką Bezpieczeństwa i równocześnie zobowiązują się do stosowania zasad w nich zawartych.

Upoważnieni pracownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

Niniejsza „Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Hotelu Kosmowski" wchodzi w życie z dniem podpisania ich prze Dyrektora Hotelu Kosmowski.