

## POLITYKA BEZPIECZEŃSTWA

**Administrator Danych** Właściciel/Dyrektor Hotelu..... dnia .....  
w podmiocie o nazwie Hotel.....zgodnie z Rozporządzeniem 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/WE (ogólne rozporządzenie o ochronie danych - RODO) wprowadza dokument o nazwie „Polityka Bezpieczeństwa”.

### § 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Hotelu..... określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

### § 2

Ilekoć w „Polityce Bezpieczeństwa” jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,

### § 3.

Administrator Danych w podmiocie Hotel..... wyznacza Inspektora Ochrony Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w Rozporządzeniu 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/WE (ogólne rozporządzenie o ochronie danych), chyba że Administrator Danych sam wykonuje te czynności.

### § 4.

Administrator Danych (lub osoba przez niego upoważniona) dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

### § 5.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych. Administrator Danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Danych nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie upoważnienia oraz prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie, w szczególności:

1. Ewidencję osób przetwarzających dane posiadających upoważnienie.
2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

### § 6.

Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany w terminie 30 dni poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

## § 7.

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

## § 8.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

## § 9.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa” mają zastosowanie odpowiednie przepisy Rozporządzenia 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/WE (ogólne rozporządzenie o ochronie danych - RODO).

## § 10.

### **Deklaracja intencji, cele i zakres polityki bezpieczeństwa**

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
5. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu

danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.
7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
  - a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
  - b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
  - c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
  - d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.
8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
  - a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
  - b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
  - c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
  - d) monitorowanie zastosowanych środków ochrony;
  - e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
  - f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.
9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów RODO.

Podpis Administratora Danych Osobowych