Załącznik nr1do zarządzenia nr [..]

z dnia [..] r.

Dom Zdrojowy
ul. Zdrojowa 2
80-515 Gdańsk

Polityka Ochrony

Danych Osobowych

Dokument wewnętrzny

Data wdrożenia: […] 2022 r.

Administrator danych osobowych

Trójmiejska Grupa Cateringowa Maciej Zdanowski

*Poszanowanie określonych zasad w niniejszej Polityce Ochrony Danych Osobowych stanowi podstawę należytego przetwarzania danych osobowych w Domu Zdrojowym ul. Zdrojowa 2, 80-515 Gdańsk*****

Spis treści

PREAMBUŁA

Polityka Ochrony Danych Osobowych została opracowana dla Domu Zdrojowego ul. Zdrojowa 2, 80-515 Gdańsk **** na podstawie i w oparciu o przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [dalej RODO].

Polityka Ochrony Danych Osobowych jest zbiorem dokumentów określających zasady dotyczące zapewnienia bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych metodą tradycyjną oraz informatyczną, które obowiązują uczestników procesów przetwarzania danych osobowych dokonujących czynności przetwarzania w ramach świadczenia pracy na podstawie różnych form współpracy na rzecz Domu Zdrojowego ul. Zdrojowa 2, 80-515 Gdańsk.

W zakresie powyższej deklaracji Administrator kieruje się najważniejszymi filarami ochrony danych osobowych w Domu Zdrojowym ul. Zdrojowa 2, 80-515 Gdańsk, na podstawie których jest opracowany system ochrony danych osobowych:

1. Podejmuje wszelkie działania niezbędne dla zapewnienia ochrony praw i usprawiedliwionych interesów każdej osoby związanych z bezpieczeństwem jej danych osobowych.
2. Stale podnosi świadomość oraz kwalifikacje osób przetwarzających dane osobowe w zakresie konieczności zapewnienia bezpieczeństwa tych danych.
3. Doskonali i rozwija nowoczesne metody zabezpieczenia gromadzonych danych osobowych przed zagrożeniami związanymi w związku z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
4. Traktuje obowiązki zatrudnionych osób oraz pracowników przetwarzających dane osobowe jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich prawidłowego wykonywania.

W zakresie powyższej deklaracji Administrator kieruje się najważniejszymi filarami ochrony danych osobowych w Domu Zdrojowym ul. Zdrojowa 2, 80-515 Gdańsk ****, na podstawie których jest opracowany system ochrony danych osobowych:

1. Legalność – Administrator dba o ochronę prywatności i przetwarza dane oraz operacje na nich przy zachowaniu pełnej zgodności z obowiązującymi przepisami prawa.
2. Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.
3. Prawa Jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw związanych z ochroną danych osobowych i prawa te realizuje.
4. Rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
5. Podejście oparte na ryzyku – Administrator identyfikuje ryzyka towarzyszące przetwarzaniu danych osobowych oraz ustala ich wpływ na operacje związane z danymi osobowymi, a w szczególności na prawa i wolności osób fizycznych;

Ponadto Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

a) w oparciu o podstawę prawną i zgodnie z prawem [legalizm];
b) rzetelnie i uczciwie (rzetelność);
c) w sposób przejrzysty dla osoby, której dane dotyczą [transparentność];
d) w konkretnych celach i niepobieranie danych „na zapas" [minimalizacja];
e) nie więcej niż potrzeba [adekwatność];
f) z dbałością o prawidłowość danych [prawidłowość];
g) nie dłużej niż potrzeba [czasowość];
h) zapewniając odpowiednie bezpieczeństwo danych [bezpieczeństwo].

I. POSTANOWIENIA OGÓLNE POLITYKI OCHRONY DANYCH OSOBOWYCH.

§1 Cel i zakres stosowania Polityki

1. Niniejszy dokument, zwany dalej „Polityką ochrony danych osobowych" stanowi zestaw wymogów, zbiorów zasad, regulacji i procedur odnoszących się do wszystkich danych osobowych przetwarzanych przez Dom Zdrojowy ul. Zdrojowa 2, 80-515 Gdańsk, których podstawowym celem jest zapewnienie w szczególności:
   a) ochrony danych osobowych przetwarzanych u Administratora przez osoby upoważnione w systemie tradycyjnym oraz w systemie informatycznym;
   b) zabezpieczenia danych osobowych przetwarzanych u Administratora przed dostępem osób nieuprawnionych;
   c) ochrony danych osobowych przetwarzanych u Administratora przed ich zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem przepisów prawa oraz przed zmianą, utratą, uszkodzeniem lub zniszczeniem;
   d) prawidłowości wykonywania obowiązków w zakresie zabezpieczenia danych osobowych, zgodnych z wymogami obowiązujących aktów prawnych odnoszących się do podmiotu.
2. Niniejszy dokument stanowi wykonanie obowiązku, o którym mowa w art. 24 ust. 2 RODO.
3. Polityka znajduje zastosowanie do wszystkich procesów przetwarzania danych osobowych u Administratora, a także ma zastosowanie do wszelkich czynności stanowiących przetwarzanie danych osobowych, bez względu na źródło pochodzenia danych, ich zakres, cel zebrania, sposób przetwarzania i okres przetwarzania.
4. Polityka znajduje zastosowanie do danych powierzonych przez Administratora do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz do danych osobowych, które zostały przez Administratora udostępnione.
5. Obowiązek ochrony danych osobowych przetwarzanych u Administratora, a tym samym obowiązek przestrzegania niniejszej Polityki, odnosi się do wszystkich osób, które mają do nich dostęp bez względu na zajmowane stanowisko, miejsce wykonywania pracy, jak również prawną formę świadczenia pracy, tj. zarówno zatrudnionych u Administratora na podstawie umowy o pracę oraz świadczących na jego rzecz usługi w oparciu o umowę cywilnoprawną czy też na podstawie innej umowy stażu, praktyki.
6. Ponadto dokument ten określa granice dopuszczalnego zachowania wszystkich użytkowników procesów przetwarzania oraz opis konsekwencji, jakie mogą ponieść przekraczając te granice.
7. Bezpośredni nadzór nad przetwarzaniem i przestrzeganiem zasad ochrony danych osobowych przez Hotel sprawuje tzw. najwyższe kierownictwo, które również nadzoruje aktualność niniejszej Polityki.
8. Aktualizacja Polityki winna nastąpić:

- w szczególności w przypadku zmiany przepisów, wydania nowych wytycznych organu nadzorczego lub Europejskiej Rady Ochrony Danych;
- gdy okaże się, że aktualne postanowienia Polityki pozostają nieadekwatne do stopnia wymaganego u Administratora.

9. Zatwierdzenie niniejszej Polityki wraz z jej załącznikami oraz jej dalsze aktualizacje następuje w drodze wydania wewnętrznej uchwały.
10. Polityka została opracowana w oparciu o obowiązujące przepisy prawa regulujące zasady przetwarzania danych osobowych osób fizycznych, tym samym realizując konstytucyjne oraz europejskie prawo każdej osoby do ochrony życia prywatnego.
11. Polityka winna być interpretowana w zgodzie z aktualnie obowiązującymi przepisami. Wszelkie wątpliwości interpretacyjne winny być rozstrzygane przy pełnym poszanowaniu zasad ochrony danych osobowych wskazanych w Preambule Polityki.

§2 Regulacje prawne

Przepisy prawa obecnie obowiązujące:
1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz. U. 1997.78.483) art. 47 określający zasady ochrony życia prywatnego oraz art. 51 określający zakaz ujawniania informacji dotyczących danej osoby.
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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);
3. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz. U z 2018 r. poz. 1000) - stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku.
4. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) – czyli tzw. „ustawy wdrożeniowej RODO".

§3 Definicje

Zastosowane w niniejszej Polityce ochrony danych osobowych zwroty oznaczają:
1. **Administrator** [w skrócie AD] – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2. **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej [„osobie, której dane dotyczą"]; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej [„osobie, której dane dotyczą"]; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. **Eksport danych –** oznacza to przekazanie danych przetwarzanych do państwa trzeciego lub organizacji międzynarodowej poza obszar Unii Europejskiej [UE] i/lub Europejski Obszar Gospodarczy [EOG];
4. **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
6. **Incydent bezpieczeństwa informacji** – rozumie się przez to zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych;

7. **Informatyk** – rozumie się przez to osobę powołaną przez Administratora lub osobę, z którą została nawiązana współpraca do pełnienia obowiązków w odniesieniu do systemów informatycznych i nadzoru nad informacją [aktywami] funkcjonującą w tych systemach informatycznych;
8. **Inspektor Ochrony Danych** [w skrócie IOD, Inspektor] **–** rozumie się przez to osobę wyznaczoną przez Administratora zarządzeniem do pełnienia funkcji Inspektora Ochrony Danych na podstawie art. 37 RODO.
9. **Integralność danych** – oznacza to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10. **Naruszenie ochrony danych osobowych** – oznacza to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
11. **Notyfikacja** – rozumie się przez to obowiązek Administratora zgłoszenia do organu nadzorczego poważnych przypadków naruszeń, gdy to naruszenie bezpieczeństwa prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
12. **Obszar przetwarzania pomieszczenia** – rozumie się przez to pomieszczenia lub części pomieszczeń we wszystkich lokalizacjach Administratora, w których są przetwarzane dane osobowe, zarówno w formie papierowej, jak i w systemie informatycznym.
13. **Odbiorcy danych –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane 4. 5. 2016 L 119/33 Dziennik Urzędowy Unii Europejskiej PL osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
14. **Ograniczenie przetwarzania** – należy przez to rozumieć oznaczenie czasowe przechowywanych danych osobowych w celu ograniczenia [zminimalizowania] ich przetwarzania w przyszłości;
15. **Organ nadzorczy** – rozumie się przez to Urząd Ochrony Danych Osobowych tzw. UODO, który jest organem kontrolującym przestrzeganie przepisów prawa w zakresie ochrony danych osobowych; Organ ten reprezentowany jest przez Prezesa Urzędu [w skrócie PUODO];
16. **Osoba –** oznacza to podmiot danych - osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
17. **Osoba upoważniona** – osoba upoważniona do przetwarzania danych osobowych przez Administratora lub osobę przez niego upoważnioną, mająca bezpośredni dostęp do danych, przetwarzanych w systemie informatycznym lub w dokumentacji papierowej.
18. **Państwo trzecie** – rozumie się przez to państwo spoza Unii Europejskiej [UE] oraz spoza do Europejskiego Obszaru Gospodarczego [EOG];
19. **Pełnomocnictwo** – rozumie się przez to dokument wydany przez Administratora w celu formalnego reprezentowana go przez wskazaną osobę [np. Dyrektora Hotelu] w zakresie zadań i czynności określonych w dokumencie, a wykonywanych w jego imieniu;
20. **Podmiot przetwarzający** [procesor] **–** oznacza to organizację lub osobę, której Administrator powierza przetwarzanie danych osobowych [np. w zakresie wypełniania obowiązków Inspektora ochrony danych, usług teleinformatycznych – domeny, hostingowych itp.];
21. **Polityka –** oznacza to niniejszą Politykę ochrony danych osobowych zawierającą zestaw praw, zasad i procedur dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych o ile co innego nie wynika wyraźnie z kontekstu
22. **Poufność danych** – oznacza to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom lub podmiotom;
23. **Profilowanie –** oznacza to 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;
24. **Przetwarzanie danych osobowych** – oznacza to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany taka jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

25. **Pseudonimizacja** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
26. **Rozliczalności** – oznacza to właściwość zapewniającą, że działania osoby na danych osobowych mogą być przypisane w sposób jednoznaczny tylko tej osobie, nadto właściwość zapewniająca możliwość udowodnienia realizacji praw osób, których dane osobowe są przetwarzane;
27. **Rozporządzenie UE** – oznacza to 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) [w skrócie RODO].
28. **Ryzyko** – rozumie się przez to kombinację prawdopodobieństwa zdarzenia i jego konsekwencji [skutków];
29. **System przetwarzania danych –** oznacza to wykorzystywany w celu przetwarzania danych osobowych system informatyczny i system tradycyjny;
30. **System informatyczny** – oznacza to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych osobowych, także w przypadku przetwarzania danych poza zbiorem danych;
31. **System tradycyjny** – oznacza to zespół procedur organizacyjnych związanych z przetwarzaniem danych osobowych na nośnikach papierowych, w tym m.in. w kartotekach, segregatorach, księgach, wykazach i w innych zbiorach ewidencyjnych;
32. **Środki techniczne i organizacyjne** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
33. **Upoważnienie** – rozumie się przez to dokument w formie papierowej stanowiący dowód, iż każda osoba mająca dostęp do danych osobowych, przetwarza je wyłącznie z upoważnienia i na polecenie Administratora lub podmiotu przetwarzającego;
34. **Ustawa –** rozumie się przez to Ustawę o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz. U. z 2018 r. poz. 1000).
35. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub ich modyfikację, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą;
36. **Uwierzytelnianiu** – oznacza to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby lub podmiotu.
37. **Użytkowniku systemu przetwarzania danych –** oznacza to pracownika Administratora lub każdą inną osobę, która odbyła stosowne szkolenie w zakresie ochrony tych danych i posiada upoważnienie udzielone przez Administratora do przetwarzania danych osobowych w systemie przetwarzania danych osobowych oraz posiada konto w systemie informatycznym należącym do Administratora;
38. **Zabezpieczeniu danych w systemie informatycznym** – oznacza to wdrożone i eksploatowane środki techniczne i organizacyjne zapewniające ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem;
39. **Zastępca Inspektora Ochrony Danych [w skrócie ZIOD lub Zastępca IOD]** – rozumie się przez to osobę wyznaczoną przez Administratora zarządzeniem do pełnienia funkcji Zastępcy Inspektora Ochrony Danych na podstawie zasad określonych w art. 11 a Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych;
40. **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
41. **Zgodzie osoby, której dane osobowe dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

II. SYSTEM PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH

§1 Obszar przetwarzania danych osobowych

1. Administrator, którym jest Trójmiejska Grupa Cateringowa Maciej Zdanowski ul. Lazurowa 8, 80 -680 Gdańsk dla hotelu wskazuje, iż dane osobowe są przetwarzane w Domu Zdrojowym ul. Zdrojowa 2, 80-515 Gdańsk **** i ustanawia wykaz miejsc i pomieszczeń, w których dochodzi do przetwarzania danych osobowych wraz z uwzględnieniem ich zabezpieczeń fizycznych.

2. Ponadto obszarem przetwarzania danych osobowych dla Hotelu może być tzw. podmiot przetwarzający, o ile Administrator przekaże dane osobowe takiemu podmiotowi, który na jego rzecz i w jego imieniu będzie przetwarzał powierzone dane osobowe.

Załącznik nr 1 *do niniejszej Polityki:*

- *Wykaz miejsc i pomieszczeń przetwarzania danych osobowych.*
- *Wykaz umów powierzenia przetwarzania danych osobowych.*

§2 Inwentaryzacja danych osobowych

1. Administrator, tj. Trójmiejska Grupa Cateringowa Maciej Zdanowski ul. Lazurowa 8, 80-680 Gdańsk dokonuje szczegółowo identyfikacji procesów przetwarzania danych osobowych polegającej na zebraniu pełnej informacji o wszystkich operacjach przetwarzania wykorzystujących dane osobowe, które wykonywane są w każdym obszarze przetwarzania Administratora ze szczególnym uwzględnieniem i odnoszących się do:
   - danych osobowych przetwarzanych na podstawie art. 6 ust. 1 lir. a) – f) RODO;
   - danych osobowych szczególnych kategorii na podstawie art. 9 RODO [tzw. danych wrażliwych] i danych osobowych dotyczących wyroków skazujących i naruszeń prawa na podstawie art. 10 RODO [tzw. danych karnych];
   - danych osobowych poddanych profilowaniu i zautomatyzowanemu podejmowaniu decyzji z uwzględnieniem przypadków przetwarzania danych osobowych;
1. Ponadto Administrator kontroluje przetwarzanie danych niezidentyfikowanych, o których mowa w art. 11 ust. 1 RODO, w szczególności w odniesieniu do nagrań [wizualnych, dźwiękowych czy audiowizualnych], korespondencji elektronicznej i wszelkich innych strumieni, które potencjalnie mogą zawierać dane osobowe.
2. Administrator w ramach dokonywanej inwentaryzacji procesów przetwarzania danych osobowych w celu zapewnienia pełnej kontroli i bezpieczeństwa nad przetwarzanymi danymi osobowymi prowadzi wykazy i ewidencje, które szczegółowo odnoszą się do wąskiej części obszarów i są pomocne w ich monitorowaniu.

§3 Procesy przetwarzania danych osobowych

1. Administrator, tj. Trójmiejska Grupa Cateringowa Maciej Zdanowski ul. Lazurowa 8, 80-680 Gdańsk określenia występujące u niego zbiory danych osobowych z uwzględnieniem formy przetwarzania danych osobowych w danym zbiorze zarówno w postaci papierowej jak i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury tych zbiorów.
2. Administrator inwentaryzuje procesy przetwarzania danych osobowych zachodzące u niego do wskazanych w Rozporządzeniu tj. RODO podstaw prawnych [art. 6 ust. 1 lir. a) – f) RODO, art. 9 RODO, art. 10 RODO] przypisując do nich określone czynności przetwarzania danych.
3. Ponadto Administrator kontroluje przetwarzanie danych niezidentyfikowanych, o których mowa w art. 11 ust. 1 RODO, w szczególności w odniesieniu do nagrań [wizualnych, dźwiękowych czy audiowizualnych], korespondencji elektronicznej i wszelkich innych strumieni, które potencjalnie mogą zawierać dane osobowe.
4. Administrator okresowo dokonuje przeglądów określonych zbiorów danych osobowych, a także procesów przetwarzania danych w szczególności pod katem:
   a) celów przetwarzania danych, w tym realizowanych czynności;
   b) kategorii osób, których dane są przetwarzane;
   c) zakresów przetwarzanych danych;
   d) podmiotów przetwarzających, którym dane są powierzane;
   e) odbiorców danych, którym dane są udostępniane.
5. Mając na uwadze zachodzące zmiany dotyczące samego procesu przetwarzania jak i przetwarzanych zbiorów danych osobowych, jak również oprogramowania wykorzystywanego w procesie przetwarzania tych danych w systemach informatycznych załącznik ten nr 2 powinien być na bieżąco analizowany i aktualizowany w przypadku jakichkolwiek operacji na danych osobowych w zbiorach, procesach tj. tworzeniu, zmianie zakresu, usuwaniu. Powyższe działania dotyczą również zmian w oprogramowaniu, które je obsługuje.
6. Administrator podejmuje decyzję o potwierdzeniu istnienia zbioru danych osobowych i procesu przewarzania. W tym celu może on dokonywać konsultacji m.in. z osobą ds. informatycznych lub pracownikami uczestniczącymi w danym procesie, czy przetwarzających dane w nowo określonym zbiorze danych.

Załącznik nr 2 *do niniejszej Polityki:*

- *Wykaz zbiorów danych oraz wykaz procesów przetwarzania danych w odniesieniu do przesłanek art. 6 ust 1, art. 9 i 10 RODO*

§4 Podstawy prawne przetwarzania danych osobowych

1. Administrator ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes określony w art. 6 ust.1 lit f) RODO, ma obowiązek znać konkretny realizowany przetwarzaniem interes Administratora, czyli swój oraz wskazać prawnie uzasadnione interesy, legalizujące przetwarzanie danych osobowych na tejże podstawie.
2. Administrator jest zobowiązany przetwarzać dane osobowe wyłącznie w oparciu o konkretną podstawę prawną oraz jest zobowiązany również w odniesieniu do każdej czynności przetwarzania danych osobowych zidentyfikować i zweryfikować podstawę prawną przetwarzania tych danych i tym samym jest zobowiązany monitorować zmiany legislacyjne i w miarę konieczności aktualizować podstawy prawne. Następnie dokumentować podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania wskazując podstawę prawną [zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel/interes].
3. Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne, np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis prawa, artykuł, czy inne dokumenty, jak: umowę, porozumienie administracyjne, gdy podstawą są żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, gdy uzasadniony cel – wskazując na konkretny interes jak np.: dochodzenie i obrona roszczeń, bezpieczeństwo i ochrona mienia.
4. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek znać podstawy prawne, w oparciu, o które przetwarzają dane osobowe u Administratora.
5. Administrator wdraża metody zarządzania pozyskanymi i już posiadanymi zgodami co umożliwia ich, np. weryfikację, czy rejestrację cofnięcia wyrażonej zgody i rejestrację podobnych czynności, jak np.: sprzeciw, ograniczenie do dalszego przetwarzania danych osobowych przetwarzanych na podstawie wcześniej wyrażonej zgodzie;
6. Przetwarzanie danych osobowych na podstawie zgody może się odbywać tylko wówczas, gdy nie ma innej podstawy przetwarzania danych osobowych. Nie należy uzyskiwać zgody na przetwarzanie danych osobowych związanych z zawarciem i wykonaniem umowy lub w odniesieniu do takich danych osobowych, których obowiązek przetwarzania wynika z przepisów prawa. Przed podjęciem decyzji o przetwarzaniu danych osobowych na podstawie zgody Administrator jest zobowiązany zweryfikować, czy dane osobowe są adekwatne do założonego celu przetwarzania.
7. Warunki i zasady związane z pobieraniem zgód oraz dalsze ich zarządzanie przez AD:

a) zabronione jest wywieranie przymusu uzyskania zgody, w szczególności poprzez odmowę wykonania umowy w przypadku niewyrażenia zgody na przetwarzanie danych osobowych;
b) zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie ją odróżnić od pozostałych kwestii;
c) zgoda musi być sformułowana w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
d) zgoda może być cofnięta w każdym momencie. Administrator zapewnia, aby wycofanie zgody było równie proste, jak jej wyrażenie;
e) przetwarzając dane osobowe na podstawie przesłanki zgody określa się i przedkłada podmiotowi danych [osobie]: cel przetwarzania, zakres, kategorie osób przetwarzających dane osobowe zgodnie z art. 13 ust. 1–2 [oraz jeśli występuje również informacje zgodnie z art. 26 ust. 2] rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. tzw. RODO;
f) dane po uzyskaniu zgody nie mogą być przetwarzane poza celem i zakresem określonym przez Administratora oraz niezgodnie z treścią deklaracji na etapie uzyskania zgody;
g) Administrator jest zobowiązany zapewnić zarządzanie zgodami, który pozwoli zweryfikować, czy dana osoba udzieliła zgody na przetwarzanie danych osobowych, czy i kiedy ją wycofała;
h) Administrator może prowadzić wykaz zgód w formie elektronicznej lub w innej według przyjętej wewnętrznie formuły w celu lepszej realizacji praw podmiotu danych dla właściwego zarządzania i kontroli na danymi, na które zgoda została i nie została wyrażona.

§5 Środki ochrony danych osobowych

1. Administrator w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych wdraża i nadzoruje odpowiednie środki w Domu Zdrojowym ul. Zdrojowa 2, 80-515 Gdańsk, które są niezbędne do osiągniecia tego celu w zakresie:

a) środków organizacyjnych dotyczących rozwiązań w celu lepszego zarządzania i nadzorowania, weryfikowania przestrzegania zasad wdrożonych w zakresie ochrony danych osobowych. Celem wprowadzenia takich

środków jest to, aby zapewniały przejrzystość reguł zabezpieczających przetwarzane dane np.: upoważnienia do przetwarzania danych osobowych, przeprowadzenie szkoleń dla osób przetwarzających dane osobowe, prowadzenie ewidencji upoważnień, czy niszczenie dokumentów w sposób mechaniczny za pomocą niszczarek dokumentów zawierających dane osobowe itp.

b) środków technicznych dotyczących zabezpieczania systemów i komputerów oraz stanowiących ochronę zawartą w oprogramowaniu, sprzęcie komputerowym i urządzeniach telekomunikacyjnych itd.: oprogramowanie antywirusowe, podtrzymania zasilania UPS, firewall itd.

c) środków fizycznych dotyczących zabezpieczeń odnoszących się do części zewnętrznej budynku i pomieszczeń oraz zabezpieczeń dokumentów i nośników z danymi w tych miejscach, aby utrudnić ich naruszenie itd.: zastosowany system monitoringu wizyjnego, alarm, kraty w oknach, drzwi zamykane na zamek, szafy metalowe itd.

***Załącznik nr 3** do niniejszej Polityki:*
- ❖ *Wykaz zastosowanych środków ochrony danych osobowych*

§6 Rejestr czynności i kategorii czynności przetwarzania danych osobowych

1. Administrator ma obowiązek prowadzenia następujących poniżej wskazanych rejestrów przy zastrzeżeniu braku takiego obowiązku, gdy Administrator zatrudnia mniej niż 250 osób, chyba że przetwarzanie, którego dokonuje może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10:

- rejestr czynności przetwarzania [RCP] danych osobowych zgodnie z wymaganiami art. 30 ust. 1 RODO, w stosunku do danych, których jest Administratorem;
- rejestr kategorii czynności przetwarzania [RKCP] danych osobowych zgodnie z wymaganiami art. 30 ust. 2 RODO, w stosunku do danych, których Administrator jest podmiotem przetwarzającym.

2. Administrator lub podmiot przetwarzający udostępniają rejestr na żądanie organu nadzorczego.
3. Podmiot przetwarzający, którym administrator powierzył dane osobowe w ramach zawartej umowy powierzenia są zobowiązane do prowadzenia rejestru kategorii czynności przetwarzania.

Załącznik nr 4 do niniejszej Polityki:
- ❖ *Rejestr Czynności Przetwarzania [RCP] danych osobowych*

***Załącznik nr 5** do niniejszej Polityki:*
- ❖ *Rejestr Kategorii Czynności Przetwarzania [RKCP] danych osobowych*

§7 Czasowe ograniczenie przetwarzania danych osobowych

1. Dane osobowe zbierane w ramach procesów przetwarzania danych osobowych realizowanych przez Administratora są przetwarzane przez czas określony przez właściwe przepisy prawa lub ustalony termin przez Administratora przy zachowaniu zasad ochrony danych osobowych.
2. Za określenie odpowiednich czasów retencji danych osobowych w procesach przetwarzania danych u Administratora odpowiada on sam poprzez wdrożenie mechanizmów kontroli tzw. cyklu życia danych osobowych w tym weryfikacji dalszej przydatności tych danych względem określonych terminów w zakresie niezbędności celu Administratora dla ich przetwarzania.
3. Ustanie celu przetwarzania danych jest równoznaczne z koniecznością zaprzestania przetwarzania danych osobowych.
4. Dane osobowe przetwarzane wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody.
5. Osoby upoważnione do przetwarzania danych osobowych powinny ściśle współpracować z Administratorem w zakresie określenia czasów retencji przetwarzanych danych osobowych.

***Załącznik nr 6** do niniejszej Polityki:*
- ❖ *Procedura anonimizacji i niszczenia dokumentów z danymi osobowymi wraz z wykazem retencji danych osobowych.*

§8 Eksport danych osobowych

1. Administrator, jeśli zachodzi takie przekazanie odnotowuje przypadki eksportu danych poza Europejski Obszar Gospodarczy [EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia] lub do organizacji międzynarodowych oraz zapewnienia zgodne z prawem warunki takiego przekazywania.
2. Niemniej jednak osoba, której dane mają zostać przekazane poza EOG zawsze zostaje poinformowana przed przekazaniem jej danych osobowych.

§9 Domyślna ochrona danych osobowych i w fazie projektowania

1. Administrator zarządza zmianami mającymi wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania zarówno w fazie projektowej ochrony danych osobowych [privacy by design] jak i w domyślnej ochronie danych osobowych [privacy by default].
2. Zasada privacy by design obowiązuje nie tylko w kontekście nowych procesów przetwarzania danych, ale w dalszym etapie zarządzania i przetwarzania danymi osobowymi przechodzi w domyślną ochronę tych danych i jako zasada privacy by default jest nadal stosowana przez cały okres trwania danego procesu. To oznacza, że prowadzony jest w tym zakresie stały monitoring wdrożonych środków ochrony danych osobowych. W razie konieczności, Administrator musi być przygotowany na wdrożenie nowych środków lub aktualizację tych, które wdrożył przy rozpoczęciu procesu przetwarzania.
3. Dodatkowo przed rozpoczęciem przetwarzania danych osobowych, czyli przed planowanym wdrożeniem procesu związanego z przetwarzaniem danych osobowych, Administrator, bazując na podejściu opartym na ryzyku, powinien ocenić wdrożenia jakich środków technicznych i organizacyjnych będzie wymagało planowane przetwarzanie, by stosowane rozwiązania były zgodne z przepisami rozporządzenia i chroniły prawa osób, których przetwarzane dane dotyczą.
4. Przed wdrożeniem nowego procesu przetwarzania danych osobowych, Administrator zwłaszcza powinien rozważyć przeprowadzenie oceny skutków dla ochrony danych czyli tzw. DPIA – data protection impact assessement).

III. PODMIOTY TWORZĄCE SYSTEM PRZETWARZANIA DANYCH OSOBOWYCH I ODPOWIEDZIALNE ZA SYSTEM

§1 Uczestnicy systemu przetwarzania danych osobowych

1. Za przetwarzanie danych osobowych u Administratora na czas opracowania niniejszej Polityki zgodnie z postanowieniami Rozporządzenia z 27 kwietnia 2018 roku [RODO] oraz Ustawy o ochronie danych osobowych z dnia 10 maja 20218 roku [ODO] oraz przepisami ustaw sektorowych oraz niniejszej Polityki odpowiadają:

- Administrator;
- Inspektor Ochrony Danych i Zastępca Ochrony Danych;
- Informatyk;
- Osoby upoważnione do przetwarzania danych osobowych;
- Podmioty przetwarzające dane osobowe na podstawie art. 28 RODO;
- Inni odbiorcy danych osobowych.

§2 Administrator

1. Zgodnie z definicją określoną w art. 4 RODO Administratorem jest Trójmiejska Grupa Cateringowa Maciej Zdanowski ul. Lazurowa 8, 80-680 Gdańsk.
2. Administrator w procesie przetwarzania danych osobowych jest odpowiedzialny za:

- zapewnienie odpowiednich środków organizacyjnych i technicznych celem przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych, a także celem zapewnienia odpowiedniego stopnia bezpieczeństwa odpowiadającego istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą;
- wdrożenie odpowiednich procedur ochrony danych osobowych;
- zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą;
- prowadzenie, jeśli jest zasadne rejestru czynności przetwarzania danych osobowych;
- prowadzenie, jeśli jest zasadne rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora;
- współpracę z organem nadzorczym;

- sprawowanie kontroli i nadzoru nad przestrzeganiem zasad i procedur przetwarzania danych osobowych w hotelu z uwzględnieniem kryterium celowości, adekwatności i zgodności z prawem;
- zawiadomienie o naruszeniu ochrony danych osobowych właściwego organu nadzorczego w ciągu 72 godzin, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, zgłoszenie osobie, której dane dotyczą;
- rejestrowanie wszelkich naruszeń ochrony danych osobowych, w tym dokumentowanie okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych;
- zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, w sytuacji, gdy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, w przypadku, gdy zajdą ku temu odpowiednie przesłanki, podejmuje konsultacje z organem nadzorczym;
- przeprowadzanie oceny skutków dla ochrony danych – DPIA;
- dopuszczanie do przetwarzania danych wyłącznie osób posiadających upoważnienie;
- nadawanie upoważnień do przetwarzania danych osobowych osobom dopuszczonym do przetwarzania danych osobowych w zbiorach hotelu;
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w formie elektronicznej i/ lub papierowej;
- zapewnienie, aby osoby upoważnione do przetwarzania danych zapoznały się z przepisami o ochronie danych osobowych w tym odbyły szkolenie z zakresu ochrony danych osobowych;
- zapewnienie, jeśli występuje, legalności przekazywania danych osobowych do podmiotów trzecich;
- zapewnienie legalności przetwarzania danych osobowych;
- prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych i nadzorowanie jej aktualizacji oraz przestrzeganie zasad w niej określonych;
- decydowanie oraz nadzorowanie i dbanie o zgodne z prawem udostępnianie i/lub przekazanie zbiorów danych osobowych [udostępnianie i powierzanie]:
  - ✓ udostępnienie danych osobowych podmiotom uprawnionym do ich otrzymania na mocy odrębnych przepisów prawa - branżowych [nadrzędnych], które regulują te kwestie lub osobom, których dane osobowe dotyczą;
  - ✓ powierzanie do dalszego przetwarzania dane osobowe na podstawie art. 28 RODO;
- respektowanie prawa osób, których dane dotyczą poprzez spełnianie obowiązku informacyjnego zgodnie przestawieniem informacji na podstawie art. 13 i 14 RODO zasadnie do pozyskiwanych danych osobowych [bezpośrednio lub pośrednio];
- wyjaśnianie wszystkich zgłoszonych nieprawidłowości i incydentów;
- zapewnienie bezpieczeństwa w sieci komputerowej;
- zapewnienie użytkownikom odpowiednich dostępów do danych osobowych przetwarzanych w systemie informatycznym umożliwiający im bezpieczne przetwarzanie danych w celu realizacji zadań [nadawanie, zmiany lub pozbawianie uprawnień dostępu do systemu informatycznego użytkowników];
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe i inne dane chronione;
- wyznaczenie, jeśli jest zasadność Inspektora Ochrony Danych i jego Zastępcy.

<u>Zobowiązania Administratora wobec Inspektora i Zastępcy Inspektora Ochrony Danych</u>:

- dokonuje czynności wyznaczenia osoby do pełnienia funkcji Inspektora Ochrony Danych oraz osobę do pełnienia funkcji Zastępcy Inspektora Ochrony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania swoich zadań przez osobę;
- wydaje wewnętrzne zarządzenie, którym wyznacza osobę do pełnienia funkcji Inspektora Ochrony Danych oraz funkcji Zastępcy Inspektora Ochrony Danych, a następnie do 14 dni od daty wydania zarządzenia informuje Urząd Ochrony Danych Osobowych o danych kontaktowych wyznaczonych Inspektorów podając ich imiona, nazwiska oraz nadany do kontaktu z Inspektorami adres e-mail;
- zobowiązany jest również do opublikowania w/w rodzaju danych kontaktowych Inspektorów na prowadzonej przez siebie stronie internetowej oraz podania tych danych do wiadomości pracowników/ współpracowników;
- nadzoruje działania Inspektora i je go Zastępcy poprzez ścisła z nimi współpracę;
- każdorazowo dokonuje ostatecznej akceptacji najważniejszych działań Inspektora Ochrony Danych i jego Zastępcy z perspektywy organizacji, w które zaangażowane są podmioty trzecie, przy zachowaniu i poszanowaniu pełnej niezależności Inspektorów;

- wspieranie Inspektora oraz jego Zastępcę w wypełnianiu przez nich zadań, o których mowa art. 39 RODO, zapewniając zasoby niezbędne do wykonania tych zadań oraz środki i organizacyjną odrębność Inspektorowi Ochrony Danych oraz jego Zastępcy w celu należnego wykonywania przez niego zadań. W tym celu Administrator dodatkowo może powołać osobę do kontaktów z Inspektorami oraz zespół do współpracy w zakresie przeprowadzania szacowania i analizy ryzyka i monitorowania procesów przetwarzania;
- umożliwia dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania wiedzy fachowej przez Inspektora oraz przez jego Zastępcę;
- zapewnia, by Inspektor oraz jego Zastępca był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
- gwarantuje, by Inspektor oraz jego Zastępca nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań;
- informuje Inspektora oraz jego Zastępcę zgłoszeniach dotyczących realizacji praw osób w zakresie przetwarzania ich danych osobowych przez Administratora;

§3 Inspektor Ochrony Danych i Zastępca Inspektora Ochrony Danych

1. Inspektor Ochrony Danych oraz jego Zastępca od momentu wyznaczenia:
- podlega bezpośrednio Administratorowi co oznacza, iż jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych z uwzględnieniem fazy privacy by design i default;
- wypełniania postanowienia swoich zadań określonych w art. 39 RODO.
2. Jeżeli u Administratora nie wyznaczono Inspektora Ochrony Danych, to poza swoimi zadaniami i obowiązkami realizuje on również zadania i obowiązki określone w art. 39 RODO odnoszące się do IOD.
3. Wyznaczenie Inspektora Ochrony Danych:
- Administrator podjął decyzję o wyznaczeniu Inspektora Ochrony Danych na podstawie art. 37 ust. 1 lit. b) RODO z uwagi na fakt, iż dochodzi u niego w sposób ciągły do przetwarzania danych osobowych i w związku z tym chce zapewnić nadzór nad przestrzeganiem przepisów, ich weryfikowania we właściwy sposób.
- Wyznaczenie IOD następuje w drodze wydania wewnętrznego i następnie zgłoszenia osoby pełniącej tą funkcję do organu nadzorczego.
4. Wyznaczenie Zastępcy Inspektora Ochrony Danych:
- Administrator może na stałe lub na czas chwilowego zastępstwa wyznaczyć zastępcę IOD, na zasadach określonych w art. 11 a Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych, co pozwala zapewnić ciągłość wykonywanych zadań IOD, ale też ze względu na to, że osoba taka musi mieć odpowiednie, takie jak IOD przygotowanie merytoryczne [zgodnie z art. 11a ust. 1 ustawy o ochronie danych osobowych] może stanowić realne i ciągłe wsparcie Administratora [i w przypadku stałego zastępstwa obsługującego go IOD].
- Wyznaczenie Zastępcy IOD następuje w drodze wydania wewnętrznego zarządzenia i następnie zgłoszenia osoby pełniącej tą funkcję do organu nadzorczego.
5. Statut Inspektora Ochrony Danych i jego Zastępcy:
- Inspektor Ochrony Danych oraz Zastępca podlegają bezpośrednio Administratorowi, tj. Trójmiejskiej Grupie Cateringowej Maciej Zdanowski ul. Lazurowa 8, 80-680 Gdańsk
- W związku z tym faktem w schemacie organizacyjnym Administratora, Inspektor Ochrony Danych i Zastępca Inspektora Ochrony Danych zostają umiejscowieni bezpośrednio w podległości Administratora, któremu składane są raporty i wskazywane zalecenia do realizacji, aby przetwarzanie danych osobowych Hotelu odbywało się zgodnie z prawem i w sposób bezpieczny dla ochrony i wolności osób, w których danych osobowych posiadaniu jest Hotel.
- Inspektor i jego Zastępca jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych z uwzględnieniem fazy privacy by design i default.
6. Inspektor Ochrony Danych oraz Zastępca IOD otrzymują od Administratora imienne upoważnienie do przetwarzania danych osobowych.

Załącznik nr 7.1 *do niniejszej Polityki:*
- ❖ *Upoważnienie dla Inspektora Ochrony Danych*

Załącznik nr 7.2 *do niniejszej Polityki:*
- ❖ *Upoważnienie dla Zastępcy Inspektora Ochrony Danych*

7. Zadania Inspektora Ochrony Danych:

- zadania IOD zostały określone w art. 39 RODO [odnoszą się również do Zastępcy IOD w przypadku jego wyznaczenia] i należą do nich:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
d) współpraca z organem nadzorczym [Urząd Ochrony Danych Osobowych];
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

- ponadto Inspektor Ochrony Danych oraz wyznaczony Zastępca Inspektora Ochrony Danych wypełniają swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;

a) zobowiązuje się do zachowania tajemnicy lub poufności co do wykonywania swoich zadań zgodnie z prawem Unii lub prawem państwa członkowskiego;
b) stanowi punkt kontaktowy dla osób, których dane osobowe przetwarza Administrator w zakresie wszystkich spraw związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO [zgodnie z art. 38 ust. 4] i w tym celu udziela ustnych lub pisemnych wyjaśnień;
c) wspiera Administratora w udzielaniu odpowiedzi do wniosków nadesłanych w zakresie zapytań o przetwarzanie danych osobowych;
d) doradza i zaleca rozwiązania w celu jak najlepszego zabezpieczania przetwarzania danych osobowych przez Administratora;
e) obsługuje dedykowaną dla niego jako Inspektora elektroniczną skrzynkę pocztową, która jest punktem kontaktowym zarówno dla osób, których dane przetwarza Administrator, jak i dla organu nadzorczego;

- do kontroli stanu ochrony danych osobowych w formie przeprowadzanych audytów, sprawdzeń, inspekcji poza samym Administratorem, upoważniony jest wyznaczony zarówno Inspektor Ochrony Danych jak i Zastępca Inspektora Ochrony Danych.

§4 Informatyk

1. Informatyk jest odpowiedzialny za nadzorowanie prawidłowego funkcjonowania sprzętu, oprogramowania i jego konserwację, a także za koordynowanie techniczno-organizacyjnej obsługi systemów informatycznych w szczególności służących do przetwarzania danych osobowych.
2. Przetwarzanie danych osobowych dokonywane jest przez Informatyka na podstawie imiennego upoważnienia wydanego przez Administratora.

Załącznik nr 8 *do niniejszej Polityki:*

❖ *Upoważnienie dla Informatyka*

3. Do obowiązków tej osoby należy:

a) nadzór nad stosowaniem Polityki Ochrony Danych Osobowych w zakresie bezpieczeństwa teleinformatycznego oraz Polityki Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych wdrożonymi do stosowania u Administratora.
b) kontrolowanie przestrzegania przez pracowników procedur bezpieczeństwa systemów informatycznych;
c) wdrażanie mechanizmów ochrony informacji przetwarzanej i przechowywanej na serwerach, komputerach stacjonarnych i komputerach przenośnych;
d) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemów informatycznych;
e) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe i inne dane chronione;

f) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, szkodliwego lub nielegalnego oprogramowania;
g) w przypadku stwierdzenia naruszenia ochrony systemu podjęcie natychmiastowych działań zabezpieczających dowody oraz funkcjonowanie systemu informatycznego;
h) w przypadku stwierdzenia naruszenia ochrony systemu analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa systemów informatycznych lub informacji w nich przetwarzanych, jeśli takie wystąpiło;

b) sporządzenie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania danych;
c) dbanie o niezakłócone działanie kluczowych aplikacji służących do przetwarzania danych;
d) sprawdzanie sposobów zabezpieczenia danych osobowych w systemach informatycznych, a w szczególności sprawdzanie:

- ✓ metod kontroli dostępu do danych przetwarzanych w systemach informatycznych;
- ✓ zastosowanych środków ochrony danych osobowych przed utratą na skutek awarii systemu informatycznego, w tym zasilania w energię elektryczną;
- ✓ zastosowanych zabezpieczeń przed zagrożeniami pochodzącymi z sieci publicznej;
- ✓ zapewnienie rozliczalności wykonywanych operacji w zakresie administrowanych systemów;
- ✓ nadzór nad środkami zapewniającymi poufność danych osobowych przetwarzanych przy wykorzystaniu elektronicznych, przenośnych nośników informacji.

§5 Osoba upoważniona

1. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora i tylko w celu wykonywania nałożonych na nią obowiązków.
2. Osoba dopuszczona do przetwarzania danych osobowych wykonuje czynności przetwarzania na podstawie wydanego jej imiennego upoważnienia do przetwarzania danych osobowych.

Załącznik nr 9 *do niniejszej Polityki:*

- ❖ *9.1 Upoważnienie do przetwarzania danych osobowych na podstawie umowy o pracę wraz z oświadczeniem osoby upoważnionej – [wzór]*
- ❖ *9.2 Upoważnienie do przetwarzania danych osobowych na podstawie umowy zlecenie, o dzieło oraz inne formy [staż, praktyka] wraz z oświadczeniem osoby upoważnionej – [wzór]*
- ❖ *9.3 Odwołanie upoważnienia do przetwarzania danych osobowych – [wzór]*

3. Upoważnienie wydaje Administrator, który prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja może być prowadzona w formie elektronicznej i/lub papierowej i podlega bieżącej aktualizacji.
4. Administrator może wydać pełnomocnictwo Dyrektorowi Hotelu w zakresie nadawania osobom upoważnionym upoważnień do przetwarzania danych osobowych, prowadzenia ewidencji oraz w reprezentowania Administratora podczas kontroli organu nadzorczego, a także do zatwierdzania i wdrażania wewnętrznych dokumentów dla Hotelu w zakresie ochrony danych osobowych.
   Nadane pełnomocnictwo zostaje wpisane w ewidencję.

Załącznik nr 10 *do niniejszej Polityki:*

- ❖ *Pełnomocnictwo do reprezentowania Administratora do wykonywania w jego imieniu niektórych zadań i obowiązków w zakresie ochrony danych osobowych – [wzór]*

Załącznik nr 11 *do niniejszej Polityki:*

- ❖ *Ewidencja osób upoważnionych do przetwarzania danych osobowych zatrudnionych na umowę w podziale na zakładki do upoważnień wydanych dla osób zatrudnionych na umowę o pracę oraz na podstawie innych form współpracy oraz pełnomocnictw – [wzór]*

5. Osoby upoważnione pisemnie do przetwarzania danych osobowych oświadczają, że zobowiązują się do zachowania w tajemnicy danych osobowych oraz do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa i przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres upoważnienia, a także po jego zakończeniu, ustaniu. Również po okresie ustania umowy [o pracę, zlecenie i inną umowę] łączącej osobę upoważnioną z Administratorem.
6. Naruszenie przez osoby upoważnione procedur bezpiecznego przetwarzania danych osobowych, w szczególności świadome udostępnienie danych osobie nieuprawnionej, lub przetwarzanie danych wobec braku podstaw, jest ciężkim naruszeniem zasad bezpiecznego przetwarzania danych osobowych i może być podstawą do podjęcia przez Administratora wobec osoby dopuszczającej się nieprawidłowości decyzji prawnych.
7. Osoby upoważnione zobowiązują się do:

- zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami Polityki służącymi do przetwarzania danych osobowych.
- stosowania określonych przez Administratora procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
- odpowiedniego zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym;
- zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą;
- nieudostępniania danych osobowych osobom nieupoważnionym;
- podporządkowanie się poleceniom Administratora w zakresie ochrony danych osobowych;
- niezwłocznego zgłaszania wszelkich przypadków naruszeń przepisów w zakresie bezpieczeństwa danych osobowych;
- zachowywania danych osobowych w tajemnicy-poufności;

8. Osoby, które nie mają w zakresie swoich obowiązków przetwarzania danych osobowych nie otrzymują upoważnień, a jedynie składają oświadczenie o zachowaniu danych osobowych w poufności w przypadku ewentualnego zapoznania się z danymi osobowymi.

Załącznik nr 12 *do niniejszej Polityki:*

❖ *Oświadczenie o zachowaniu poufności*

§6 Podmioty przetwarzające

1. Administrator może powierzyć innemu podmiotowi przetwarzanie danych osobowych jedynie w drodze umowy lub innego instrumentu prawnego, określonego na podstawie zapisów w art. 28 RODO.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych osobowych w imieniu Administratora jest poddanie weryfikacji podmiotu w zakresie przestrzegania i wdrożenia przez niego zasad ochrony danych osobowych analizie, która to powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji bezpieczeństwa i ochrony powierzonych w przetwarzanie danych osobowych.
3. Zakazane jest korzystanie z usług podmiotów przetwarzających, które takich gwarancji nie dają.
4. Każdorazowe skorzystanie z usług podmiotu przetwarzającego obydwa się na podstawie zawartej umowy powierzenia przetwarzania danych osobowych.

Załącznik nr 13 *do niniejszej Polityki:*

❖ *Umowa powierzenia przetwarzania danych osobowych*

5. Umowa powierzenia może zostać zawarta również w formie elektronicznej.
6. Podmiot, któremu zostały powierzone dane, może przetwarzać dane wyłącznie w określonym celu i zakresie. Każdy przypadek powierzenia danych osobowych Administrator rejestruje w rejestrze, wykazie podmiotów przetwarzających.
7. Umowa powierzenia przetwarzania danych osobowych może zostać zawarta jedynie z podmiotem, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów RODO i chroniło prawa osób, których dane dotyczą. W tym celu Administrator może dokonać wyboru właściwego podmiotu przetwarzającego na podstawie wcześniejszej weryfikacji podmiotu poprzez uzyskanie informacji o stosowanych środkach bezpieczeństwa niezbędnych do przetwarzania powierzonych danych osobowych.
8. Kontrola [w tym inspekcja] podmiotów przetwarzających zgodnie z warunkami wskazanymi w zawartej pomiędzy stronami umowy lub porozumienia powierzenia przetwarzania danych należących do Administratora jest przeprowadzana przez samego Administratora lub w przypadku wyznaczenia przez Inspektora lub inne wyznaczone osoby zgodnie z zapisami zawartymi w umowach powierzenia przetwarzania danych osobowych, w odniesieniu do uprawnienia określonego w art. 28 ust. 3 lit. h RODO.

§7 Odbiorcy danych osobowych

1. Administrator przekazuje dane osobowe podmiotom przetwarzającym, które stają się odbiorcami tych danych na mocy umowy zawartej zgodnie z art. 28 RODO, Administrator realizując niniejszą Politykę dopuszcza, że dane osobowe, których jest Administratorem może lub jest zobowiązany przekazać innym administratorom w formie udostępnienia tych danych wskutek:
   - nałożonego obowiązku prawnego na Administratora – w zakresie obowiązku prawnego nałożonego na Administratora odbiorcami danych będą podmioty, którym dostęp do danych osobowych Administrator

jest zobowiązany przekazać w związku z pełnieniem roli pracodawcy i/lub zleceniodawcy co jest regulowane przepisami prawa pracy czy przepisami polityki społecznej, podatkowej itd.

Takimi odbiorcami danych będą m.in.: Zakład Usług Społecznych, zakład medycyny pracy, Urząd Skarbowy, które w zakresach udostępnionych danych są odrębnymi administratorami danych. Z tymi podmiotami Administrator [lub w jego imieniu podmiot przetwarzający, któremu zostały dane osobowe powierzone w przetwarzanie] nie zawiera umowy powierzenia przetwarzania danych ani żadnego innego porozumienia o przetwarzaniu danych osobowych, gdyż zarówno Administrator, jaki określeni powyżej przykładowi odbiorcy danych działają w ramach przepisów prawa.

- otrzymanego pisma o udostępnienie danych osobowych – zakresie danych, które mają zostać udostępnione przez Administratora w związku z nadesłanym pismem to takie udostępnienie danych może nastąpić jedynie w oparciu o co najmniej jedną z przesłanek spośród wskazanych w art. 6 RODO i/lub art. 9 RODO lub wskazanych w szczegółowych przepisach sektorowych odnoszących się do pozyskania danego zakresu danych osobowych.

Pismo, wniosek o udostępnienie danych osobowych może wpłynąć zarówno od organów działających na podstawie określonych sektorowych przepisów prawa np. policja, sąd, prokuratura, komornik sądowy, jak również od podmiotów czy osób fizycznych, które nie działają w oparciu o przepisy sektorowe, a mają prawo wnieść takie pismo, wniosek.

Niemniej jednak bez względu na fakt od kogo pochodzi pismo, wniosek o udostępnienie danych musi zawsze mieć formę pisemną i zawierać właściwą podstawę prawną na podstawie, której Administrator będzie uprawniony udostępnić dane oraz cel i zakres tych danych.

W przypadku braku takiej podstawy prawnej Administrator od razu odmawia ujawnienia danych osobowych jakiemukolwiek odbiorcy danych osobowych.

W przypadku określenia podstawy prawnej Administrator weryfikuje jej zasadność co do podania wskazanych w piśmie rodzaju i zakresie danych i pozyskaniu danych przez dany podmiot, osobę jako uprawniony do ich pozyskania. W przypadku niezgodności również udziela odpowiedzi odmownej podając jej powód.

- żądania osoby, której dane dotyczą – w przypadku udostępnienia danych na żądanie osobie, której dane dotyczą odbywa się po uprzednim dokładnym zweryfikowaniu i potwierdzeniu tożsamości tej osoby z właściwym dokumentem do okazania czy dane, które mają zostać udostępnione dotyczą właściwej osoby.

2. W przypadkach udostępnień danych osobowych poza sytuacją pierwszą Administrator powinien prowadzić wykaz udostępnionych danych w formie elektronicznej i/lub papierowej.
3. W takim wykazie uwzględnia następujące informacje:
   - rodzaj udostępnionych danych osobowych;
   - cel oraz podstawę prawną, na podstawie, której udostępniono do innego administratora dane osobowe;
   - nazwę i adres siedziby administratora, któremu udostępnione zostały dane osobowe;
   - formę za pomocą, której dane zostały udostępnione;
   - datę dokonania udostępnienia.
4. W przypadku udostępnienia danych osobowych w formie elektronicznej należy przestrzegać zasad hasłowania załączników z jednoczesnym podaniem dostępu do hasła inna drogą, niż poczta elektroniczna. Natomiast udostępnienie w formie papierowej lub na nośniku np. pendrive powinno się odbywać za pomocą protokołu zdawczo odbiorczego udostępnionych danych osobowych podpisane przez osoby reprezentujące [uprawnione] ze strony obu administratorów.

IV. POSTĘPOWANIE PRZY NARUSZENIACH OCHRONY DANYCH OSOBOWYCH

§1 Informowanie o naruszeniach ochrony danych osobowych

1. AD jest zobowiązany wdrożyć środki umożliwiające jak najszybsze wykrywanie i klasyfikowanie naruszeń ochrony danych osobowych oraz reagowanie na dostrzeżone incydenty.
2. Każda osoba, która powzięła wiedzę, niezależnie od źródła pochodzenia, o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych, zobowiązana jest do niezwłocznego poinformowania o powyższym Administratora.
3. Inspektor Ochrony Danych we wsparciu swojego Zastępcy oraz w porozumieniu z osobami, które ewentualnie uczestniczyły w identyfikacji naruszenia danych osobowych dokonuje oszacowania ryzyka i podjęcia dalszego postępowania w zakresie zastosowania natychmiastowych środków bezpieczeństwa, a następnie rozważenia zgłoszenia naruszenia organowi nadzorczemu oraz zawiadomienia osób, których dane dotyczą.

§2 Zgłaszanie naruszenia do organu nadzorczego - UODO

1. W sytuacji stwierdzenia wystąpienia naruszenia ochrony danych osobowych oraz prawdopodobieństwa zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych, informacja o naruszeniu powinna zostać zgłoszona do PUODO. W sytuacjach wątpliwych lub niejednoznacznych należy dokonać zgłoszenia do PUODO.
2. Zgłoszenia naruszenia dokonuje sam Administratorem w terminie 72 godzin po stwierdzeniu naruszenia, zgodnie z wymaganiami art. 33 RODO.
3. W przypadku, gdy naruszenie ochrony danych odnosi się do procesów przetwarzania realizowanych przez Administratora w roli podmiotu przetwarzającego, jest on zobowiązany do podjęcia adekwatnych środków zaradczych oraz do niezwłocznego poinformowania administratora powierzonych danych.
4. W sytuacji, gdy stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o naruszeniu należy zawiadomić wszystkie osoby, których dane dotyczą. Przeprowadza się w tym zakresie analizę w odniesieniu do wymogów art. 34 ust. 3 RODO.
5. Każde stwierdzone naruszenie ochrony danych osobowych, niezależnie do tego, czy jest zgłaszane do organu nadzorczego czy też nie, jest dokumentowane u Administratora.

Załącznik nr 14 *do niniejszej Polityki:*
- ❖ *Procedura obsługi naruszeń ochrony danych osobowych*

V. PRAWA PODMIOTÓW DANYCH

§1 Zasady obsługi podmiotów danych

1. Administrator spełnia obowiązki nałożone na niego przepisami RODO w zakresie:
- przekazywania osobom informacji o przetwarzaniu ich danych osobowych za pomocą stosowanych klauzul informacyjnych;
- zapewnia możliwości efektywnego wykonania każdego typu żądania przez siebie i przez podmioty, którym dane osobowe powierzył w przetwarzanie;
- zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
- zawiadamiania o naruszeniach zgodnie z stosowaną procedurą pozwalającą na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

§2 Obowiązek informacyjny

1. Administrator jest zobowiązany realizować obowiązki informacyjne, o których mowa w art. 13 RODO i art. 14 RODO względem osób, których dane osobowe przetwarza.
2. Administrator spełnia obowiązek informacyjny w przypadku pozyskania danych bezpośrednio od podmiotu danych — w chwili pozyskiwania tych danych oraz w przypadku pozyskiwania danych osobowych nie bezpośrednio od podmiotu danych:
- w rozsądnym terminie po pozyskaniu danych, jednak nie później niż w terminie miesiąca;
- najpóźniej przy pierwszej komunikacji z podmiotem danych, jeżeli dane osobowe mają być wykorzystywane do komunikacji;
- przy pierwszym ujawnieniu, jeżeli dane osobowe mają być ujawnione innemu odbiorcy.
3. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych, są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO.
4. Za stosowanie właściwych klauzul informacyjnych przy zbieraniu danych osobowych odpowiada Administrator.
5. Klauzule informacyjne muszą być umieszczone w widocznych i łatwo dostępnych miejscach dla osób, których dane dotyczą np. na stronie internetowej, w regulaminie świadczenia usług, w umowach, kwestionariuszach itd.

Załącznik nr 15 *do niniejszej Polityki:*
- ❖ *Wykaz klauzul informacyjnych*

§3 Prawa podmiotów danych

1. Każdej osobie, której dane osobowe są przetwarzane są przez Administratora zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [RODO] każda osoba, której dane są przetwarzane ma prawną możliwość skorzystania ze swoich tzw. praw osób, których dane dotyczą w zakresie:

- dostępu do treści danych [art. 15 Rozporządzenia];
- do sprostowania danych [art. 16 Rozporządzenia];
- do usunięcia danych [art. 17 Rozporządzenia];
- do ograniczenia przetwarzania danych [art. 18 Rozporządzenia];
- do przenoszenia danych [art. 20 Rozporządzenia];
- do wniesienia sprzeciwu wobec przetwarzania danych [art. 21 Rozporządzenia];
- do powiadomienia każdego odbiorcę o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, którego dokonuje sam administrator realizując swoje obowiązki [art. 19 Rozporządzenia];

  Prawa te mogą w szczególnych przypadkach podlegać ograniczeniom wynikającym z odrębnych przepisów do wycofania wyrażonej zgody [w przypadku, gdy przetwarzanie odbywa się na jej podstawie] bez wpływu na zgodność przetwarzania z prawem, którego dokonano na podstawie zgody przed jej wycofaniem [art. 7 ust. 3 Rozporządzenia].

  Ponadto osoba fizyczna, gdy uzna, iż przetwarzanie jej danych osobowych narusza przepisy Rozporządzenia przez Administratora ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych [na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa]. Więcej informacji znajduje się pod linkiem: https://uodo.gov.pl/ w zakładce Skargi.

2. Za rozpatrywanie złożonych do Administratora żądań w zakresie uprawnień, o których mowa w ust. 1, odpowiada sam Administrator.
3. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu Administrator rozpatruje indywidualnie.
4. Wobec osoby, która zgłasza żądanie związane z realizacją swoich praw wynikających z RODO Administrator wypełnia obowiązek informacyjny w związku z przetwarzaniem danych osobowych wnioskodawcy w celu wykazania wypełniania obowiązków prawnych i usprawiedliwionego interesu przez Administratora.
5. W celu należytego wypełniania realizacji praw osób Administrator może w tym celu mieć określaną wewnętrzną procedurę zgodnie, z którą postępuje w sytuacji, gdy osoba, której dane dotyczą skieruje do Administratora żądanie związane z realizacją jej praw, określonych w art. 15 – 18 i 20 - 21 RODO.

Załącznik nr 16 *do niniejszej Polityki:*

- *Procedura realizacji praw osób*

VI. MONITOROWANIE PRZESTRZEGANIA PRZEPISÓW O ROZLICZALNOŚCI ZGODNOŚCI REALIZACJI OBOWIĄZKÓW RODO

§1 Kontrola i doskonalenie systemu ochrony danych osobowych

1. W celu weryfikacji zastosowanych u Administratora środków technicznych i organizacyjnych, zapewniających przetwarzanie danych osobowych zgodnie z RODO, wykonuje się ich monitorowanie poprzez np. audyty, czy sprawdzenia przeprowadzane przez IOD i jego Zastępcę.
2. Monitorowanie w formie audytu, sprawdzeń obejmuje wszelkie procesy przetwarzania danych osobowych, zbiory danych osobowych, a także dokumentację służącą określenie zasad ochrony danych osobowych.
3. W wyniku przeprowadzonego audytu, sprawdzenia sporządzony zostaje raport, który przez IOD i/lub Zastępcę IOD następnie jest przekazywany do Administratora, który na jego podstawie inicjuje dalsze działania korygujące lub zapobiegawcze, jeśli takie zostały wskazane w raporcie.
4. Celem audytu, czy sprawdzenia czyli kontroli jest weryfikacja zasad i uporządkowanie ich oraz przedstawienie rozwiązań związanych z bezpieczeństwem danych osobowych.
5. Zastrzega się, iż w przypadku poważnego naruszenia ochrony danych osobowych audyt wewnętrzny przeprowadzany jest niezwłocznie po usunięciu skutków naruszenia.

§2 Analiza ryzyka

1. Administrator, wdrażając odpowiednie środki techniczne i organizacyjne, uwzględnia stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub

wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia po to, aby przetwarzanie odbywało się zgodnie z RODO i aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2. Analizę ryzyka należy dokonywać cyklicznie, w razie zmiany charakteru, zakresu, kontekstu lub celu przetwarzania, w razie przetwarzania danych w nowym celu.
3. Analizę ryzyka wykonuje się w oparciu o wcześniej opracowaną procedurę i przyjętą metodologię do szacowania ryzyka.
4. W przypadku, gdy analiza ryzyka wykaże umiarkowane, wysokie lub bardzo wysokie ryzyko naruszenia praw lub wolności osób fizycznych konieczne jest niezwłoczne podjęcie adekwatnych środków minimalizujących ryzyko.
5. Administrator stosuje zabezpieczenia danych osobowych dostosowane do aktualnego stopnia ryzyka.

§3 Ocena skutków dla ochrony danych

1. Administrator przeprowadza Ocenę skutków dla ochrony danych [DPIA] w przypadku realizacji procesów przetwarzania danych osobowych u siebie, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania zgodnie z art. 35 RODO, ale także gdy jest konieczne w przypadkach określonych w art. 35 ust. 3 i 4 RODO.
2. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby nie zostały zastosowane środki w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy skonsultować się z organem nadzorczym.
3. W przypadku konieczności przeprowadzenia konsultacji z organem nadzorczym należy skierować wniosek o konsultacje do UODO zgodnie z art. 36 RODO i skontaktować się w tej sprawie z organem nadzorczym.

§4 Szkolenia

1. Każda osoba przetwarzająca dane osobowe w formie papierowej i/lub informatycznej musi być poddana przeszkoleniu z zakresu ochrony danych osobowych przed przystąpieniem do przetwarzania danych osobowych.
2. Za organizację szkolenia odpowiada Administrator, który inicjuje ich potrzebę.
3. Szkolenia powinna przeprowadzać osoba posiadająca wymagane kwalifikacje i mająca wiedzę z zakresu przepisów ochrony danych osobowych również w kontekście innych przepisów krajowych.
4. Szkolenia przeprowadza wyznaczony Inspektor Ochrony Danych oraz jego Zastępca.
5. Dopuszczalne jest, aby pierwsze szkolenie osoba przed dopuszczeniem jej do przetwarzania danych osobowych odbyła w formie samokształcenia poprzez zapoznanie się z instruktarzem wstępnym przygotowanym przez Inspektora Ochrony Danych lub jego Zastępcę, a następnie odbywa szkolenie w formie stacjonarnej lub online.
6. Każde następne szkolenie przypominające w tym odnoszące się do dalszych szczegółowych zagadnień związanych z ochroną danych osobowych było przeprowadzane w formie stacjonarnej, samokształcenia się lub w formie online z wykorzystaniem komunikatora internetowego.
7. Każde przeprowadzone szkolenie z zasad ochrony danych osobowych musi zostać udokumentowane przez osobę je przeprowadzającą tj. IOD.
8. Administrator zapewnia osobom przez siebie zatrudnionym szkolenia z zakresu ochrony danych osobowych, których częstotliwość oraz stopień zaawansowania zależy od pozycji uczestnictwa w systemie ochrony danych osobowych [szkolenia uzupełniające, stanowiskowe] jednak każda osoba przetwarzająca dane osobowe przynajmniej raz w roku musi odbyć szkolenie przypominające z zakresu ochrony danych osobowych.

I. POSTANOWIENIA KOŃCOWE

§1 Przestrzeganie Polityki i odpowiedzialność

1. Przestrzeganie Polityki Ochrony Danych Osobowych i sankcje karne:

- wszelkie zasady opisane w niniejszym dokumencie – Polityce Ochrony Danych Osobowych oraz w załącznikach do niej są przestrzegane przez wszystkie osoby będące pracownikami i współpracownikami [zleceniobiorcami, praktykantami, stażystami] Administratora jako mających dostęp do informacji zbieranych, przetwarzanych i przechowywanych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą, bez względu na zajmowane stanowisko oraz miejsce wykonywania powierzonych przez Administratora czynności i zadań jak również charakter nawiązanej współpracy z Administratorem;

- przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu w zakresie opisanych zasad, procedur odnoszących się do zabezpieczania i należytego przetwarzania danych osobowych mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych;
- wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa przetwarzania danych osobowych i zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła określonych działań wskazanych w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby o tym fakcie, będą podjęte dalsze działania. Osoba musi być świadoma swojej odpowiedzialności za takie działanie;
- wobec osób winnych dopuszczenia się uchybień mających w konsekwencji narażenie Administratora na kary finansowe, prestiżowe i kontrolne, oprócz postępowania dyscyplinarnego, może zostać wszczęte postępowanie dyscyplinarne lub inne postępowanie przewidziane prawem;

§2 Zmiany w dokumentacji Polityki Ochrony Danych Osobowych

1. Polityka ODO zawiera zasady ochrony danych. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych osobowych, zmiany prawa lub konieczność uaktualnienia pewnych zapisów może być dokumentem dynamicznie zmieniającym się w czasie.
2. Na polecenie Administratora dokument ten może być zmieniony lub uzupełniony, aby parametry stosowanych przy przetwarzaniu danych osobowych zabezpieczeń i procedur znajdowały na bieżąco odzwierciedlenie funkcjonalne w niniejszym dokumencie, jednak w sposób nie zmieniający stopnia ochrony danych osobowych.
3. Wszelkie zmiany dokonywane w Polityce Ochrony Danych Osobowych muszą być wprowadzone odrębnym zarządzeniem zmieniającym zapisy w dokumencie i odnotowane w odrębnym wykazie zmian odnoszącym się do niniejszego dokumentu z określeniem jakie zapisy zostały dodane lub usunięte, czy zmodyfikowane.

§3 Regulacje końcowe

1. Polityka wraz z dołączonymi do niej załącznikami jest dokumentem wewnętrznym, stanowiącym tajemnicę przedsiębiorstwa i nie może być udostępniana osobom nieupoważnionym w żadnej formie, chyba że obowiązek jej udostępnienia ma charakter prawny.
2. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO, UODO oraz odpowiednich ustaw sektorowych.
3. Administrator określa zakres dostępu do treści niniejszego dokumentu oraz do jego załączników do zapoznania się przez osoby upoważnione do przetwarzania danych osobowych.
4. W celu zapewnienia ochrony danych osobowych dostęp do załączników posiadają osoby zgodnie z posiadanym upoważnieniem Administratora.
5. Administrator może opracowywać i wdrażać odrębne procedury i polityki w zakresie danych osobowych w celu usprawnienia systemu zarządzania i przetwarzania posiadanych w zbiorach Administratora danymi osobowymi.
6. Na polecenie Administratora niniejszy dokument ten może być zmieniony lub uzupełniony, aby parametry stosowanych przy przetwarzaniu danych osobowych zabezpieczeń i procedur znajdowały na bieżąco odzwierciedlenie funkcjonalne w niniejszym dokumencie, jednak w sposób nie zmieniający stopnia ochrony danych osobowych.
7. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody Administratora. Dokument może być udostępniony osobom i instytucjom postronnym za zgodą Administratora, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych, a wszelkie załączniki występują w formie niewypełnionych szablonów.
8. Polityka obowiązuje od dnia jej zatwierdzenia przez Administratora.

Wykaz załączników do Polityki:

Załącznik nr 1 do niniejszej Polityki
– 1.1_Wykaz miejsc i pomieszczeń przetwarzania danych osobowych
– 1.2_Wykaz umów powierzenia przetwarzania danych osobowych

Załącznik nr 2 do niniejszej Polityki
– Wykaz zbiorów danych oraz wykaz procesów przetwarzania danych w odniesieniu do przesłanek art. 6 ust 1, art. 9 i 10 RODO

Załącznik nr 3 do niniejszej Polityki
– Wykaz zastosowanych środków ochrony danych osobowych

Załącznik nr 4 do niniejszej Polityki
– Rejestr czynności przetwarzana danych osobowych

Załącznik nr 5 do niniejszej Polityki
– Rejestr kategorii czynności przetwarzana danych osobowych

Załącznik nr 6 do niniejszej Polityki
– Procedura anonimizacji i niszczenia dokumentów z danymi osobowymi

Załącznik nr 7 do niniejszej Polityki
– 7.1_Upoważnienie dla Inspektora Ochrony Danych
– 7.2_Upoważnienie dla Zastępcy Inspektora Ochrony Danych

Załącznik nr 8 do niniejszej Polityki – Upoważnienie dla Informatyka

Załącznik nr 9 do niniejszej Polityki
– 9.1_Upoważnienie do przetwarzania danych osobowych na podstawie umowy o pracę wraz z oświadczeniem osoby upoważnionej – [wzór]
– 9.2_Upoważnienie do przetwarzania danych osobowych na podstawie umowy zlecenie oraz inne formy [staż, praktyka] wraz z oświadczeniem osoby upoważnionej – [wzór]
– 9.3_Odwołanie upoważnienia do przetwarzania danych osobowych – [wzór]

Załącznik nr 10 do niniejszej Polityki – Pełnomocnictwo do reprezentowania Administratora do wykonywania w jego imieniu niektórych zadań i obowiązków w zakresie ochrony danych osobowych – [wzór]

Załącznik nr 11 do niniejszej Polityki – Ewidencja osób upoważnionych do przetwarzania danych osobowych zatrudnionych na umowę w podziale na zakładki do upoważnień wydanych dla osób zatrudnionych na umowę o pracę oraz na podstawie innych form współpracy oraz pełnomocnictw – [wzór]

Załącznik nr 12 do niniejszej Polityki – Oświadczenie o zachowaniu poufności

Załącznik nr 13 do niniejszej Polityki – Umowa powierzenia przetwarzania danych osobowych

Załącznik nr 14 do niniejszej Polityki – Procedura obsługi naruszeń ochrony danych osobowych

Załącznik nr 15 do niniejszej Polityki – Wykaz klauzul informacyjnych.

Załącznik nr 16 do niniejszej Polityki – Procedura realizacji praw osób