POLITYKA OCHRONY DANYCH OSOBOWYCH

CENTRUM MEDYCZNE MULTIMED spółka z ograniczoną odpowiedzialnością, Al. Z Krasińskiego 9/24B, 31--111 Kraków, NIP: 676 248 40 40, REGON: 360616015, KRS: 0000540401;

Centrum Medyczne Multimed
Os. Władysława Jagiełły 15
32-800 Brzesko

I. POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka Ochrony danych osobowych, (dalej: Polityka Ochrony) w firmie CENTRUM MEDYCZNE MULTIMED spółka z ograniczoną odpowiedzialnością, Al. Z Krasińskiego 9/24B, 31--111 Kraków, NIP: 676 248 40 40, REGON: 360616015, KRS: 0000540401;, Centrum Medyczne Multimed, Os. Władysława Jagiełły 15, 32-800 Brzesko (dalej: MULTIMED) powstała w związku z koniecznością dostosowania dotychczasowej polityki bezpieczeństwa danych osobowych do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

Niniejsza Polityka Ochrony określa zasady ochrony przetwarzania danych osobowych, jakie powinny być przestrzegane i stosowane w MULTIMED przez osoby zatrudnione oraz współpracujące z MULTIMED, które przetwarzają dane osobowe.

II. PODSTAWA PRAWNA PRZETWARZANIA

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

III. ZAKRES STOSOWANIA

1. Niniejszą Politykę Ochrony stosuje się do wszelkich danych osobowych osób fizycznych przetwarzanych przez MULTIMED, w tym danych osobowych przetwarzanych w systemie informatycznym, danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
2. W zakresie podmiotowym, Polityka Ochrony obowiązuje wszystkich pracowników MULTIMED, osoby zatrudnione na umowy cywilnoprawne oraz inne osoby i podmioty mające dostęp do danych osobowych.
3. Informacje niejawne nie są objęte zakresem niniejszej Polityki Ochrony.
4. Niniejsza Polityka Ochrony zawiera:
   a) opis zasad ochrony danych obowiązujących w MULTIMED;
   b) odwołania do załączników uszczegóławiających.

IV. OCHRONA DANYCH OSOBOWYCH W MULTIMED – ZASADY OGÓLNE

1. Ochrona danych osobowych w MULTIMED – zasady ogólne

1.1 Zasady ochrony danych osobowych w MULTIMED:

a) **Legalność** − MULTIMED dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

b) **Bezpieczeństwo** − MULTIMED zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

c) **Prawa Jednostki** − MULTIMED umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

d) **Rozliczalność** − MULTIMED dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2.1 Zasady ochrony danych

MULTIMED 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 nie „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).

V. OSOBY ODPOWIEDZIALNE W MULTIMED ZA OCHRONĘ DANYCH

1. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest MULTIMED, a w ramach firmy:

a) **Dyrektor do spraw administracyjnych,** któremu powierzono nadzór nad obszarem ochrony danych osobowych;
b) osoba wyznaczona przez MULTIMED do zapewnienia zgodności z ochroną danych osobowych;

za nadzór i monitorowanie przestrzegania Polityki odpowiadają:

c) **Inspektor Ochrony Danych**, jeżeli został powołany w MULTIMED;
d) **komórka audytu wewnętrznego**, jeżeli funkcjonuje w MULTIMED;

za stosowanie niniejszej Polityki odpowiedzialni są:

e) MULTIMED;
f) wszystkie komórki organizacyjne;
g) wszyscy członkowie personelu MULTIMED.

MULTIMED powinna też zapewnić zgodność postępowania kontrahentów MULTIMED z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez MULTIMED.

2. **Dyrektor do spraw administracyjnych**, któremu powierzono nadzór nad obszarem ochrony danych osobowych odpowiedzialny jest za:

a) zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych;
b) zapoznanie podległych pracowników i osoby zatrudnione na podstawie umów cywilnoprawnych z treścią RODO, Polityką Ochrony w zakresie przetwarzania danych osobowych, Instrukcją w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz instrukcją postępowania w sytuacji naruszenia danych osobowych;
c) nadzór nad poprawnością realizacji przepisów rozporządzenia, w szczególności zasad opisanych w Polityce Ochrony oraz Instrukcji, oraz nad wykonaniem zadań związanych z ochroną danych osobowych;

d) podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych;
e) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych,
f) wprowadzanie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;
g) egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych;
h) poddawanie przeglądom skuteczność Polityki Ochrony danych osobowych;
i) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;
j) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
k) zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych

VI. DEFINICJE

Użyte w Polityce Ochrony definicje oznaczają:
Administrator Danych – CENTRUM MEDYCZNE MULTIMED spółka z ograniczoną odpowiedzialnością, Al. Z Krasińskiego 9/24B, 31--111 Kraków, NIP: 676 248 40 40, REGON: 360616015, KRS: 0000540401, podmiot, który decyduje o środkach i celach przetwarzania danych osobowych, zwany dalej MULTIMED;
Administrator Systemów Informatycznych (ASI) – osoba fizyczna lub osoba prawna zarządzająca systemem informatycznym w MULTIMED (zazwyczaj osoba fizyczna zatrudniona na stanowisku informatyka);
Polityka - oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu;
RODO - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);
Dane - oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;
Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
Możliwa do zidentyfikowania osoba fizyczna - 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
Dane wrażliwe - oznaczają dane specjalne i dane karne;
Dane specjalne - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
Dane karne - oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;

Dane dzieci - oznaczają dane osób poniżej 16. roku życia;
Instrukcja - Instrukcja Zarządzania Systemem Informatycznym obowiązująca MULTIMED;
Kierownictwo – Zarząd, organ zarządzający i reprezentujący Administratora Danych, prokurent samoistny;
Osoba - oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
Podmiot przetwarzający - oznacza organizację lub osobę, której MULTIMED powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość);
Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
Przetwarzanie danych osobowych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
Eksport danych - oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
Zbiór danych -uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
Zabezpieczanie danych osobowych – środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;
Usuwanie danych osobowych – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
IOD lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych;
RCPD lub Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych;
Przedsiębiorca - oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym MULTIMED, spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

VII. SYSTEM OCHRONY DANYCH

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

1) **Inwentaryzacja danych.** MULTIMED dokonuje identyfikacji zasobów danych osobowych w MULTIMED klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   a) przypadków przetwarzania danych specjalnych i danych „kryminalnych" (**dane wrażliwe**);
   b) przypadków przetwarzania danych osób, których MULTIMED nie identyfikuje (**dane niezidentyfikowane**/UFO);
   c) przypadków przetwarzania danych dzieci;
   d) profilowania;
   e) współadministrowania danymi.

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

3) **Podstawy prawne.** MULTIMED zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
   a) utrzymuje system zarządzania zgodami na przetwarzanie danych;
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy MULTIMED przetwarza dane na podstawie prawnie uzasadnionego interesu MULTIMED.

4) **Obsługa praw jednostki.** MULTIMED spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne.** MULTIMED przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b) **Możliwość wykonania żądań.** MULTIMED weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   c) **Obsługa żądań.** MULTIMED zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
   d) **Zawiadamianie o naruszeniach.** MULTIMED stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** MULTIMED posiada zasady i metody zarządzania minimalizacją a w tym:
   a) zasady zarządzania **adekwatnością** danych;
   b) zasady reglamentacji i zarządzania **dostępem** do danych;
   c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** MULTIMED zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
   d) posiada system zarządzania bezpieczeństwem informacji;
   e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

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

8) **Eksport danych.** MULTIMED posiada zasady weryfikacji, czy MULTIMED nie przekazuje danych do państw trzecich (t.j. poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

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

10) **Przetwarzanie transgraniczne.** MULTIMED posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

VIII. INWENTARYZACJA DANYCH

6.1. Dane wrażliwe

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

6.2. Dane niezidentyfikowane

MULTIMED identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

6.3. Profilowanie

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

6.4. Współadministrowanie

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

IX. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

7.1. Rejestr Czynności Przetwarzania Danych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7.2. MULTIMED prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

7.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających MULTIMED rozliczanie większości obowiązków ochrony danych.

7.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą MULTIMED uznała za odrębną dla potrzeb Rejestru, MULTIMED odnotowuje co najmniej:

a) nazwę czynności,
b) cel przetwarzania,
c) opis kategorii osób,
d) opis kategorii danych,
e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu MULTIMED, jeśli podstawą jest uzasadniony interes,
f) sposób zbierania danych,
g) opis kategorii odbiorców danych (w tym przetwarzających),
h) informację o przekazaniu poza EU/EOG;
i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

7.5. Wzór Rejestru stanowi **Załącznik do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”.**

X. PODSTAWY PRZETWARZANIA

a) MULTIMED dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

b) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel MULTIMED) MULTIMED dookreśla podstawę w czytelny sposób, gdy jest to potrzebne, t.j.. dla zgody wskazując na jej zakres lub przepis prawny i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

c) MULTIMED wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

d) Kierownik komórki organizacyjnej MULTIMED ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes MULTIMED, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes MULTIMED.

XI. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

a) MULTIMED dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

b) MULTIMED ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej MULTIMED informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w MULTIMED, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze MULTIMED w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

c) MULTIMED dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

d) MULTIMED wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

e) W celu realizacji praw jednostki MULTIMED zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez MULTIMED, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

f) MULTIMED dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

XII. OBOWIĄZKI INFORMACYJNE

a) MULTIMED określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

b) MULTIMED informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

c) MULTIMED informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

d) MULTIMED informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

e) MULTIMED określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

f) MULTIMED informuje osobę o planowanej zmianie celu przetwarzania danych.

g) MULTIMED informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

i) MULTIMED informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

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

XIII.

9. Żądania osób

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

b) **Nieprzetwarzanie**. MULTIMED informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

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

d) **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, MULTIMED informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych MULTIMED nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

e) **Kopie danych**. Na żądanie MULTIMED wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. MULTIMED wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

f) **Sprostowanie danych**. MULTIMED dokonuje sprostowania nieprawidłowych danych na żądanie osoby. MULTIMED ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych MULTIMED informuje osobę o odbiorcach danych, na żądanie tej osoby.

g) **Uzupełnienie danych**. MULTIMED uzupełnia i aktualizuje dane na żądanie osoby. MULTIMED ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. MULTIMED nie musi przetwarzać

danych, które są MULTIMED zbędne). MULTIMED może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez MULTIMED procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

h) **Usunięcie danych.** Na żądanie osoby, MULTIMED usuwa dane, gdy:

(1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
(2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
(3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
(4) dane były przetwarzane niezgodnie z prawem,
(5) konieczność usunięcia wynika z obowiązku prawnego,
(6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

MULTIMED określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
Jeżeli dane podlegające usunięciu zostały upublicznione przez MULTIMED, MULTIMED podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.
W przypadku usunięcia danych MULTIMED informuje osobę o odbiorcach danych, na żądanie tej osoby.

a) **Ograniczenie przetwarzania.** MULTIMED dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

(1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
(2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
(3) MULTIMED nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
(4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie MULTIMED zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania MULTIMED przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
MULTIMED informuje osobę przed uchyleniem ograniczenia przetwarzania.
W przypadku ograniczenia przetwarzania danych MULTIMED informuje osobę o odbiorcach danych, na żądanie tej osoby.

b) **Przenoszenie danych.** Na żądanie osoby MULTIMED wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, **jeśli** jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona MULTIMED, przetwarzane na podstawie zgody tej osoby lub w celu

zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych MULTIMED.

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

d) **Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.** Jeżeli MULTIMED prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. MULTIMED uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

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

f) **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli MULTIMED przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na **osobę**, MULTIMED zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie MULTIMED, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a MULTIMED; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

XIV. MINIMALIZACJA

MULTIMED dba o minimalizację przetwarzania danych pod kątem:

a) adekwatności danych do celów (ilości danych i zakresu **przetwarzania**),
b) dostępu do danych,
c) czasu przechowywania danych.

a. Minimalizacja zakresu

MULTIMED zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
MULTIMED dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
MULTIMED przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą.

b. Minimalizacja dostępu

MULTIMED stosuje ograniczenia dostępu do danych osobowych:

(1) prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń);
(2) logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
(3) kontrolę dostępu fizycznego.

MULTIMED dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

MULTIMED dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji MULTIMED.

c. Minimalizacja czasu

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

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

XV. BEZPIECZEŃSTWO

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

a. Analizy ryzyka i adekwatności środków bezpieczeństwa

MULTIMED przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(1) MULTIMED zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

(2) MULTIMED kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

(3) MULTIMED przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. MULTIMED analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

(4) MULTIMED ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym MULTIMED ustala przydatność i stosuje takie środki i podejście jak:

a) pseudonimizacja,

b) szyfrowanie danych osobowych,

c) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

d) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

b. Oceny skutków dla ochrony danych

MULTIMED dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

MULTIMED stosuje metodykę oceny skutków przyjętą w MULTIMED.

c. Środki bezpieczeństwa

MULTIMED stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w MULTIMED i są bliżej opisane w procedurach przyjętych przez MULTIMED dla tych obszarów.

d. Zgłaszanie naruszeń

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

XVI. PRZETWARZAJĄCY

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

MULTIMED przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik do Polityki – „Wzór umowy powierzenia przetwarzania danych"**.

MULTIMED rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

XVII. EKSPORT DANYCH

MULTIMED rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.
Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, MULTIMED okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

XVIII.

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

XIX. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.
2. Każda osoba mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

3. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
4. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
5. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
6. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
7. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające szczególne. Szczegółowa procedura nadawania i odwoływania upoważnień do przetwarzania danych osobowych została określona w Instrukcji.
8. Upoważnienia do przetwarzania danych osobowych, odwołania upoważnień do przetwarzania danych osobowych oraz oświadczenia, o których mowa powyżej przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.
9. Rejestr osób upoważnionych do przetwarzania danych osobowych prowadzony jest zgodnie z wytycznymi określonymi w Instrukcji.
10. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.
11. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w MULTIMED, w szczególności Polityki Ochrony oraz Instrukcji.

XX. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie PMiW prowadzi działalność. Do takich pomieszczeń, zalicza się w szczególności:
   1) pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
   2) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
   3) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
3. Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład 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 drzwi.
4. Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
5. Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek.
6. Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

7. Szczegółowy wykaz obszarów przetwarzania danych osobowych znajduje się w załączniku nr ……. do niniejszej Polityki Ochrony.
8. Pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych należy wyposażyć w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.
9. Kopie zapasowe zawierające dane osobowe należy przechowywać w drugiej fizycznej lokalizacji w bezpiecznej odległości od lokalizacji podstawowej.
10. Należy wdrożyć politykę czystego biurka i czystego ekranu w celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych. Wzór polityki czystego biurka stanowi Załącznik do niniejszej Polityki Ochrony
11. Klucze dostępowe, karty, hasła itp. służące do uzyskania dostępu do systemów informatycznych służących do przetwarzania danych osobowych należy zabezpieczać a sposób ich uzyskiwania należy szczegółowo zdefiniować w procedurach.
12. Przyznawanie dostępu gościom należy wykonywać wyłącznie w określonych i autoryzowanych celach.
13. Kończąc pracę, należy zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację, wydruki, elektroniczne nośniki informacji i umieścić je w zamykanych szafkach.

XXI. OCENA RYZYKA I PRZEGLĄDY

1. Systemy informatyczne i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych co najmniej raz na dwa lata. Ocena ryzyka powinna być również przeprowadzana przy dużych zmianach procesów biznesowych, systemów informatycznych i aplikacji.
2. Narzędzia informatyczne służące do oceny ryzyka bezpieczeństwa przetwarzania danych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.
3. Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo, co najmniej raz na 1 rok w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.
4. Przeglądy zgodności z zasadami bezpieczeństwa przetwarzania danych osobowych urządzeń informatycznych oraz sieci teleinformatycznych należy przeprowadzać okresowo, co najmniej raz na rok.
5. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa przetwarzania danych osobowych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

XXII. POSTANOWIENIA KOŃCOWE

1. Niniejsza Polityka Ochrony powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach MULTIMED, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Okresowy przegląd Polityki Ochrony powinien mieć na celu stwierdzenie, czy postanowienia Polityki Ochrony odpowiadają aktualnej i planowanej działalności MULTIMED oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

3. Zmiany niniejszej Polityki Ochrony wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w MULTIMED.
4. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Ochrony może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
5. Osoby zatrudnione w MULTIMED zobowiązane są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Ochrony. W wypadku odrębnych od zawartych w niniejszej Polityce Ochrony uregulowań występujących w innych procedurach obowiązujących w MULTIMED mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

Łukasz Grzybała
Prezes zarządu