Polityka bezpieczeństwa informacji

****

# Cel dokumentu

Wprowadzenie Polityki Bezpieczeństwa Informacji, zwanej dalej Polityką, ma na celu ustanowienie kierunku zarządzania bezpieczeństwem informacji. Polityka stanowi nadrzędny dokument Systemu Zarządzania Bezpieczeństwem Informacji. Wynikające z niej zasady pomagają rozwijać działalność MDH poprzez zapewnienie klientów oraz kontrahentów o wysokim standardzie usług realizowanych przez MDH Sp. z o.o. zwanym dalej MDH.

# Zakres dokumentu

Polityka wraz z dokumentacją powiązaną oraz wypełnianie ich postanowień obowiązuje wszystkie osoby uczestniczące w procesie przetwarzania informacji w MDH. Poszczególne regulacje podległe polityce mogą obejmować również podmioty współpracujące, przetwarzające informacje.

# Deklaracja najwyższego kierownictwa

Zarząd MDH niniejszym dokumentem deklaruje świadomość potrzeby ochrony informacji oraz wskazuje zabezpieczenia, mechanizmy i procesy to umożliwiające. Zarządzanie bezpieczeństwem informacji jest procesem podlegającym ciągłym zmianom, dlatego Zarząd rozpoznaje ciągłe doskonalenie jako istotny element systemu.

# Podstawa prawna

* 1. System Zarządzania Bezpieczeństwem Informacji (SZBI) uwzględnia regulacje prawne, którym podlega MDH, w szczególności:

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
3. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

# Definicje

* 1. Przez użyte w treści Polityki i dokumentacji powiązanej sformułowania należy rozumieć:

1. **Administrator Danych Osobowych (ADO)** – MDH Sp. z o.o., decyduje o celach i środkach przetwarzania danych osobowych. Organem realizującym obowiązki ADO jest najwyższe kierownictwo, tj. Zarząd MDH
2. **Administrator Systemu Informatycznego (ASI)** – osoba lub osoby funkcyjne wyznaczane przez Administratora Danych Osobowych odpowiedzialne za przestrzeganie i nadzór nad przestrzeganiem zasad bezpieczeństwa informacji w systemie informatycznym w zakresie przypisanych im obowiązków i uprawnień. Różne systemy mogą posiadać różnych ASI.
3. **Bezpieczeństwo informacji** – oznacza zapewnienie poufności, integralności oraz dostępności informacji.
4. **Dane „wrażliwe”** – dane osobowe objęte szczególną ochroną, wskazane w art. 9 i 10 RODO. Takimi danymi są m.in. dane o stanie zdrowia, dane daktyloskopijne, dane o wyrokach, itp.
5. **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, przy czym 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.
6. **Dostępność** – oznacza zapewnienie, że informacja jest dostępna zawsze wtedy, kiedy zachodzi taka potrzeba przez podmiot uprawniony.
7. **Incydent** – (Incydent związany z bezpieczeństwem informacji) oznacza pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
8. **Inspektor Ochrony Danych (IOD)** - osoba fizyczna wyznaczana przez Administratora Danych Osobowych monitorująca przestrzeganie przepisów o ochronie danych osobowych, zgodnie z przydzielonym zakresem obowiązków.
9. **Integralność** – oznacza właściwość zapewniającą, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany.
10. **Naruszenie ochrony danych osobowych** – oznacza 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. **Osoby upoważnione** - wszystkie osoby mające upoważnienie do przetwarzania danych osobowych, z racji wykonywanych obowiązków służbowych oraz nadanego upoważnienia lub upoważnione do przetwarzania na podstawie przepisów prawa i umów powierzenia. Osoby upoważnione są osobami uprawnionymi.
12. **Osoby uprawnione** - wszystkie osoby uprawnione do przetwarzania informacji, z racji wykonywanych obowiązków służbowych lub uprawnione do przetwarzania na podstawie przepisów prawa lub zawartych umów.
13. **Poufność** – oznacza właściwość zapewniającą, że informacje nie są udostępniane osobom trzecim.
14. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na informacjach 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.
15. **Przetwarzanie danych** - operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym.
16. **RODO -** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
17. **Struktura informatyczna** - zespół środków technicznych i ich zabezpieczeń, tj. urządzeń (komputerów, drukujące, łączności, wraz z okablowaniem i oprogramowaniem) oraz oprogramowania (systemów operacyjnych, oprogramowania urządzeń), a także sieć informatyczna i udostępniane przez nią zasoby.
18. **System informatyczny** – oznacza oprogramowanie lub grupę programów służących do przetwarzania danych w obrębie wspólnej bazy danych, w szczególności posiadające wspólne uwierzytelnianie użytkowników.
19. **System Zarządzania Bezpieczeństwem Informacji** (**SZBI)** – oznacza zbiór wszystkich zasad, procedur i procesów realizowanych w celu zapewniania bezpieczeństwa informacji.
20. **Ustawa -** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
21. **Usuwanie danych** - zniszczenie danych osobowych lub taka ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
22. **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
23. **Użytkownik** – osoba, której zostały przydzielone uprawnienia w systemie informatycznym.
24. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie.
25. **Zdarzenie** – (Zdarzenie związane z bezpieczeństwem informacji) oznacza stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

# Ogólne zasady bezpieczeństwa informacji

* 1. Podstawą Systemu Zarządzania Bezpieczeństwem Informacji oraz stosowanych zabezpieczeń są wymagania prawne, wyniki przeprowadzanego szacowania ryzyka utraty bezpieczeństwa informacji oraz wyniki monitorowania realizowanego przez IOD i audytów zewnętrznych lub wewnętrznych oraz przeglądu zarządcze.
  2. Bezpieczeństwo informacji jest realizowane poprzez stosowanie zabezpieczeń organizacyjnych, technicznych, fizycznych oraz środowiskowych.
  3. Przez informacje objęte ochroną opisaną w dokumentacji SZBI należy rozumieć dane osobowe, w rozumieniu artykułu 4 RODO.
  4. Przez zapewnienie bezpieczeństwa informacji rozumie się zapewnienie każdego z tych atrybutów informacji:

1. poufności – rozumianej jako właściwość zapewniająca, że informacje nie są udostępniane nieupoważnionym osobom,
2. integralności – rozumianej jako właściwość zapewniająca, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany,
3. dostępności – rozumianej jako zapewnienie, że informacja jest dostępna zawsze wtedy, kiedy zachodzi taka potrzeba.
   1. W MDH obowiązują następujące zasady bezpieczeństwa:
4. „Zasada wiedzy koniecznej” – osoby uprawnione posiadają informacje niezbędne do wykonywania przez nich obowiązków.
5. „Zasada potrzeby koniecznej” – osoby uprawnione mają dostęp jedynie do zasobów, które są niezbędne do wykonywania przez nich obowiązków.
6. „Zasada zachowania poufności” – osoby uprawnione są zobowiązane do zachowania poufności o informacjach, które zdobyły przez realizowanie swoich czynności zawodowych oraz o stosowanych w MDH zabezpieczeniach obejmujących te informacje.
   1. We wszystkich sytuacjach spornych lub specyficznych wymaganiach nieujętych w dokumentacji SZBI, zezwolenia na odstępstwa może wydać Zarząd lub w uzasadnionych sytuacjach bezpośredni przełożony. Sytuacje wymagające odstępstw mogą być podstawą do dalszego rozwijania dokumentacji.

# Odpowiedzialności w bezpieczeństwie informacji

## Administrator Danych Osobowych

* + 1. Zarząd (jako realizujący zadania ADO) – odpowiada za zapewnianie środków na realizowanie postanowień wynikających z wymagań prawnych, zatwierdzanie dokumentacji SZBI, przydzielanie obowiązków w zakresie bezpieczeństwa informacji oraz prowadzenie nadzoru nad zgodnością przetwarzania danych osobowych.
    2. Zarząd wyznacza Inspektora Ochrony Danych oraz Administratorów Systemów Informatycznych.
    3. Obowiązki ADO wynikające z przepisów prawa, m.in. przeprowadzanie oceny skutków, spełnianie obowiązku informacyjnego, wypełnianie praw osób, których dane dotyczą są realizowane przez wyznaczone osoby oraz zgodnie z postanowieniami dokumentacji SZBI.

## Inspektor Ochrony Danych

* + 1. Do obowiązków IOD należy:
       - monitorowanie zgodności z przepisami ochrony danych osobowych,
       - opiniowanie przeprowadzonych szacowań ryzyka oraz oceny skutków naruszeń,
       - monitorowanie dokumentacji SZBI,
       - nadzór nad przeszkoleniem osób upoważnionych do przetwarzania danych osobowych z przepisami i zasadami dotyczącymi ochrony danych osobowych,
       - doradzanie osobom upoważnionym oraz Administratorowi w kwestiach przetwarzania danych osobowych i zgodności z RODO.
    2. W celu realizacji w/w powierzonych zadań IOD ma prawo:
       - kontrolować osoby przetwarzające dane osobowe w zakresie właściwego stosowania ochrony danych osobowych w odniesieniu do SZBI oraz przepisów prawa,
       - wydawać polecenia osobom upoważnionym w zakresie bezpieczeństwa danych osobowych, w konsultacji z Zarządem, chyba że zagrożone jest bezpieczeństwo danych osobowych,
       - informować Zarząd o przypadkach naruszenia bezpieczeństwa danych osobowych,
       - żądać od wszystkich osób przetwarzających wyjaśnień, w sytuacjach naruszenia bezpieczeństwa danych osobowych oraz w celu ustalenia stanu faktycznego ochrony danych osobowych.

## Administrator Systemu Informatycznego

* + 1. ASI, w zależności od przypisanego zakresu czynności wynikającego z zatrudnienia, odpowiada za:
       - Przeprowadzanie lub nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
       - zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur, określających częstotliwość ich zmiany w systemach informatycznych,
       - nadzór nad czynnościami związanymi z prowadzeniem systemu, w zakresie obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywanych procedur uaktualnienia systemów antywirusowych i ich konfiguracji,
       - nadzór nad wykonywaniem i przechowywaniem kopii zapasowych baz danych, systemów informatycznych i innych plików,
       - nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów, służących do przetwarzania danych osobowych,
       - czuwanie nad prawidłowym działaniem podległego mu systemu informatycznego.
       - nadawania uprawnień, gromadząc wnioski od KKO dotyczące uprawniania nowych pracowników.
    2. ASI bierze udział w ocenie zdarzeń naruszających bezpieczeństwo informacji, dotyczących struktury informatycznej.
    3. W zależności od sytuacji ASI uczestniczy w ocenie skutków naruszeń oraz uczestniczy w procesie analizowania wpływu na bezpieczeństwo informacji przy wprowadzanych zmianach.

## Kierownicy komórek organizacyjnych

* + 1. Wskazane obowiązki dotyczą Kierowników komórek organizacyjnych (KKO), zespołów oraz innych pracowników pełniących obowiązki przełożonego względem danej grupy pracowników
    2. KKO odpowiadają za:
       - uczestnictwo w procesie upoważniania oraz nadawania uprawnień – w tym określanie zakresu upoważnień podległych pracowników,
       - zgłaszanie zmian w zakresie obowiązków wpływających na zakres upoważnienia lub uprawnień w systemie informatycznym,
       - nadzór nad przestrzeganiem obowiązujących zasad przez podległych pracowników,
       - uczestniczenie w procesie zarządzania incydentami – w tym zgłaszania, określania wymaganych działań oraz dalszego postępowania z incydentami,
       - uczestniczenie w określaniu wpływu zmian w MDH na bezpieczeństwo przetwarzanych informacji,
       - analizowanie zawieranych umów oraz zlecania usług podmiotom zewnętrznym pod kątem sytuacji powierzenia danych osobowych.

## Osoby uprawnione

* + 1. Osoby uprawnione, w tym osoby posiadające upoważnienie, są zobowiązane do:
       - przestrzegania przepisów prawa oraz zasad bezpieczeństwa informacji,
       - zwracanie uwagi na obce osoby, znajdujące się bez nadzoru w obszarach z ograniczonym dostępem dla osób trzecich lub w miejscach przeznaczonych dla osób uprawnionych,
       - zgłaszania zdarzeń potencjalnie naruszających bezpieczeństwo informacji,
       - zgłaszania słabości lub niepoprawnego działania stosowanych zabezpieczeń,
       - zgłaszania wszelkich zmian w zakresie procesów przetwarzania informacji lub zbiorów danych osobowych, w tym rozszerzania lub zmniejszania zakresu przetwarzanych danych, usuwania lub konieczności utworzenia nowych procesów lub zbiorów.

## Pozostali pracownicy

* + 1. Pozostali pracownicy, nie związani z przetwarzaniem informacji, są zobowiązani do:
       - zgłaszania zdarzeń potencjalnie naruszających bezpieczeństwo informacji – pozostawionych dokumentów poza zamykanymi obszarami, szafami lub otwartych pomieszczeń po godzinach pracy, itp.
       - zgłaszania źle funkcjonujących zabezpieczeń, zwłaszcza fizycznych.

# Przegląd i rozwój systemu zarządzania bezpieczeństwem informacji

* 1. Rozwój SZBI jest realizowany zgodnie z Procedurą zarządzania zmianą oraz podejmowanymi na tej podstawie działaniami udoskonalającymi.
  2. Okresowo przeprowadzane jest szacowanie ryzyka utraty bezpieczeństwa informacji zgodnie z procedurą przeprowadzania szacowania ryzyka i oceny skutków.
  3. Przegląd SZBI jest realizowany wewnętrznie, poprzez bezpośredni nadzór nad przestrzeganiem przyjętych zasad, zgodnie z podziałem obowiązków oraz w związku z realizacją procedur zarządzania incydentami oraz zarządzania zmianą.
  4. Przegląd jest również realizowany poprzez audyty wewnętrzne lub zewnętrzne, w zakresie bezpieczeństwa informacji. Źródłem informacji o stanie bezpieczeństwa są również wyniki monitorowania realizowanego przez IOD.
  5. Na potrzeby rozwoju dokumentacji SZBI oraz zapewniania jej przestrzegania, wprowadza się numery wydania. Przed wypełnieniem postanowień danej regulacji, należy zweryfikować jej aktualne wydanie, zgodnie z wykazem dokumentów powiązanych, zgodnie z punktem 9.

# Dokumenty powiązane

Polityka bezpieczeństwa informacji posiada poniższą dokumentację powiązaną:

* 1. Polityka bezpieczeństwa danych osobowych – Wydanie 1
  2. Instrukcja zarządzania systemem informatycznym – Wydanie 1
  3. Procedura zarządzania incydentami – Wydanie 1
  4. Procedura zarządzania zmianą – Wydanie 1
  5. Procedura przeprowadzania szacowania ryzyka i oceny skutków – Wydanie 1

**Dnia 25 maja 2018, Łódź Zarząd :**

Piotr Baczyński

Anetta Włodarczyk

Mariusz Gierałt