

POLITYKA PRYWATNOŚCI

PREAMBUŁA

Niniejszy dokument określa zasady ochrony danych osobowych w Hospital Investment Group Sp. z o. o., zwana dalej Administratorem.

Niniejsza Polityka jest zgodna z 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) – dalej RODO.

Polityka zawiera opis zasad ochrony danych obowiązujących u Administratora oraz wzorce procedur, instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych.

Nadzór i monitorowanie przestrzegania Polityki sprawuje powołany Inspektor Ochrony Danych Osobowych, wyznaczona do tego jednostka organizacyjna lub Administrator zgodnie z zasadami reprezentacji. Administrator powinna też zapewnić zgodność postępowania kontrahentów Administratora z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych.

Polityka ochrony danych osobowych jest w sposób systematyczny i ciągle weryfikowana i rozwijana w związku z rozwojem Administratora, podejmowanymi przez niego działaniami i rozwojem nowych technologii.

SŁOWNIK POJĘĆ UŻYTYCH W POLITYCE

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)
- **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.
- **Administrator danych (Administrator)** 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;
- **Dane osobowe** rozumie się przez to wszelkie 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.

- **Zbiór 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.

- **Przetwarzanie danych** rozumie się przez to jakiegokolwiek operacje 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.

- **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

- **Zgoda osoby, której dane dotyczą** oznacza 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;

- **Osoba upoważniona** oznacza osobę, która otrzymała od administratora danych upoważnienie do przetwarzania danych.

- **Upoważnienie** oznacza oświadczenie nadawane przez administratora danych wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu.

- **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

- **Naruszenie ochrony danych osobowych (incydent)** 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 przetwarzania.

- **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

- **IOD** oznacza Inspektora Ochrony Danych Osobowych

- **RCPD** oznacza Rejestr czynności przetwarzania danych osobowych.

ZASADY OGÓLNE OCHRONY DANYCH OSOBOWYCH

Prowadząc politykę ochrony danych osobowych Administrator kieruje się następującymi zasadami:

1. **Legalność** – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
2. **Bezpieczeństwo** – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych podejmując stale działania w tym zakresie.
3. **Prawa Jednostki** – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. **Rozliczalność** – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
5. **Czasowość i minimalizacja** – Administrator przetwarza wyłącznie te dane, które są jej niezbędne oraz nie dłużej niż jest to potrzebne
6. **Ciągłość działań** - Administrator traktuje ochronę danych osobowych jako proces, który należy stale monitorować i udoskonalać.
7. **Powszechność** – w ochronę danych zaangażowani są wszyscy pracownicy Firmy, a poszanowanie prywatności jest wpisane w codzienne działania Firmy

PODSTAWOWE MECHANIZMY OCHRONY DANYCH OSOBOWYCH STOSOWANE PRZEZ FIRMĘ

1. Administrator dokonuje identyfikacji i inwentaryzacji zasobów danych osobowych, klas danych, identyfikacji sposobów wykorzystania danych, w tym:
 - przypadków przetwarzania danych wrażliwych;
 - przypadków przetwarzania danych osób, których Administrator nie identyfikuje (dane niezidentyfikowane);
 - przypadków przetwarzania danych dzieci;
 - profilowania;
 - współadministrowania danymi.
1. Administrator opracowuje, prowadzi i aktualizuje Rejestr Czynności Danych Osobowych w Firmie.
2. Administrator identyfikuje i weryfikuje podstawy prawne przetwarzania danych w Firmie.
3. Administrator wypełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw.
4. Administrator podejmuje starania w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych, w tym:
 - przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
 - przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
 - dostosowuje środki ochrony danych do ustalonego ryzyka;
 - stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie incydentu naruszenia danych
5. Administrator powierza przetwarzanie danych wyłącznie gdy jest to konieczne dochowując staranności przy wyborze podmiotów przetwarzających oraz

- zapewniając zgodność prawem powierzenia
6. Administrator weryfikuje fakt przekazywania danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
 7. Administrator zarządza zmianami mającymi wpływ na ochronę danych osobowych. Podejmowane działania uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności już w fazie projektowania.
 8. Administrator posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

INWENTARYZACJA DANYCH

1. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych.
2. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem.
4. Administrator identyfikuje przypadki współadministrowania danymi.

PODSTAWY PRZETWARZANIA

5. Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
6. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel) Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne.

OBOWIĄZKI INFORMACYJNE

1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym powołuje dedykowany na potrzeby obsługi osób, których dane przetwarza adres e-mail _____
3. Administrator dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.
4. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.
6. Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
7. Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
8. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby, gdy jest to konieczne.

9. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej, gdy jest to konieczne.
10. Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe.
11. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych, gdy jest to konieczne.
12. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.
13. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

ŻĄDANIA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

1. Przed obsługą zgłoszenia Administrator dokonuje wiarygodnej weryfikacji, czy osoba dokonująca zgłoszenia jest uprawniona do złożenia zgłoszenia.
2. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, 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 Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
3. Na żądanie Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator 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.
4. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
5. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie musi przetwarzać danych, które są Administratorowi zbędne). Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że oświadczenie to jest niewiarygodne.
6. Na żądanie osoby, Administrator usuwa dane, gdy:
 - a. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
 - b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
 - c. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
 - d. dane były przetwarzane niezgodnie z prawem,
 - e. konieczność usunięcia wynika z obowiązku prawnego,
 - f. 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).

7. W przypadku usunięcia danych, na żądanie osoby, której dane dotyczą Administrator informuje osobę o odbiorcach danych.
8. Prawo do sprzeciwu przysługuje osobie względem przetwarzania danych do celów wynikających z prawnie uzasadnionego realizowanego przez administratora lub stronę trzecią oraz na potrzeby marketingu bezpośredniego.
9. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
10. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego (w tym **ewentualnie** profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
11. Na żądanie osoby Administrator 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 Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.
12. W przypadku skorzystania z osoby z przysługujących jej praw w zakresie danych osobowych, Administrator informuje o dokonanych operacjach na danych tę osobę.

MINIMALIZACJA

1. Administrator dba o minimalizację przetwarzania danych pod kątem: adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych, czasu przechowywania danych.
2. Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania
3. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania
4. Administrator stosuje ograniczenia dostępu do danych osobowych:
5. Administrator stosuje kontrolę dostępu fizycznego.
6. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w wewnętrznych procedurach Administratora.
7. Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych.

BEZPIECZEŃSTWO

1. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.
2. Administrator stosuje środki bezpieczeństwa dostosowane do wniosków wynikających z analiz ryzyka.
3. Stosowane przez Administratora środki bezpieczeństwa nie są ujawniane osobom niepowołanym celem zapewnienia ich skuteczności.
4. Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego incydentów naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

PRZETWARZAJĄCY

1. Administrator powierza dane osobowe wyłącznie w sytuacjach, gdy przetworzenie danych zgodnie z celem z uwagi na warunki prawne lub organizacyjne nie jest możliwe bezpośrednio przez Administratora
2. Administrator dokonuje doboru i weryfikacji przetwarzających na jego rzecz dane 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 Administratorowi.

EKSPORT DANYCH

1. Administrator rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy

PROJEKTOWANIE PRYWATNOŚCI

1. Administrator zarządza zmianami i nowymi przedsięwzięciami mającymi wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

KONTAKT

W związku z przetwarzaniem prosimy o kontakt pod adresem e-mail lub w formie pisemnej na dane: Hospital Investment Group Sp. z o. O. ul. Dąbrowskiego 77A, 60-529 Poznań
(dalej: Administrator) e-mail: iod@teleradiologia24.com.