Polityka Ochrony Danych Osobowych

w

N32 Dental Clinic

Gabinet: ul.Nowolipie 7A/U2, 00-146 Warszawa

1 Wstęp 2

2 Rejestr czynności przetwarzania (inwentaryzacja danych osobowych) 3

3 Ocena skutków (analiza ryzyka) 3

3.1 Opis operacji przetwarzania (inwentaryzacja aktywów) 3

3.2 Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO) 4

3.3 Analiza ryzyka 4

3.4 Plan postępowania z ryzykiem 6

4 Upoważnienia 6

5 Instrukcja postępowania z incydentami 6

6 Zabezpieczenia: Instrukcja zarządzania RODO 7

7 Zabezpieczenia: Regulamin Ochrony Danych Osobowych 7

8 Szkolenia 8

9 Audyty 8

10. Plan ciągłości działania 8

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Administratorem jest: N32 Dental Clinic, ul. Korfantego 14, 01-496 Warszawa, gabinet: ul. Nowolipie 7a/U2, 00-146 Warszawa, tel. 790600123, email: recepcja@n32.pl
Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

Administrator wyznaczył Inspektora Ochrony Danych, Panią Magdalenę Tomczak, email: iod@n32.pl.

DEFINICJE

Administrator(danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO–rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r.(Dz. Urz. UE L 119 z 04.05.2016)

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, szczególne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która 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.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2 REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH)

Administrator jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr będący inwentarzem danych osobowych przetwarzanych przez Administratora stanowi podstawę do przeprowadzenia analizy ryzyka. Administrator prowadzi rejestr zgodnie z załącznikiem **Rejestr czynności przetwarzania.**

3 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeśli nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

3.1 OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

W celu przeprowadzenia oceny skutków wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. W tym celu wypełniany jest **Rejestr czynności przetwarzania**

1. Rejestr czynności w wersji do udokumentowania oceny skutków powinien obejmować takie informacje, jak:

    a. opis kategorii osób,

    b. opis celów przetwarzania,

    c. charakter, zakres, kontekst danych osobowych,

    d. odbiorcy danych,

    e. funkcjonalny opis operacji przetwarzania,

    f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).

3.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec odnośnych kategorii osób.

W szczególności należy zapewnić, że:

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9),
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas (retencja danych),
4. wobec tych osób wykonano tzw. **obowiązek informacyjny** (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5. (niezależnie od konieczności przeprowadzenia oceny skutków) opracowano klauzule informacyjne dla powyższych osób,
6. (niezależnie od konieczności przeprowadzenia oceny skutków) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28) zgodnie z załącznikiem **Umowa powierzenia** (wykaz podmiotów przetwarzających prowadzony jest w załączniku **Rejestr umów powierzenia**).

3.3 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla kategorii osób lub dla procesów przetwarzania.

Uwaga: Analiza ryzyka jest wykonywana dla kategorii osób i procesów przetwarzania poddanych ocenie skutków, jednak powinna być także przeprowadzana dla wszystkich istotnych kategorii osób zawartych w RCP, np. dla kategorii osób: kandydatów do pracy, pracowników, pacjentów,

Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. Naruszenie (Incydent) ochrony danych osobowych - 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.
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent).

4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).

5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

3.3.1 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń/naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów

3.3.2 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

3.3.3 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

3.3.4 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie – przerzucenie ryzyka (outsourcing).
    b. Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji).

c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę).

3. Analizę ryzyka przeprowadza się w specjalnym szablonie **Arkusz analizy ryzyka RODO.**

3.3.5 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).

3.4 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz **Plan postępowania z ryzykiem.**
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

4 UPOWAŻNIENIA

Procedura stanowi opis postępowania w procesie kontroli dostępu do przetwarzania danych osobowych.

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych osobowych, których jest administratorem (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora.
3. Stosowane są pisemne upoważnienia ze wskazaniem czynności przetwarzania i kategorii osób, wzór w załączniku **Upoważnienie**.
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osobowych, załącznik **Ewidencja osób upoważnionych**.

5 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

Incydentem może być: przypadkowe lub niezgodne z prawem zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych)

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu Administratora lub Inspektora Ochrony Danych
2. Kontakt do w/w osoby w przypadku incydentu: Administrator: tel. 790600123, email: recepcja@n32.pl, Inspektor Ochrony danych: email: iod@n32.pl
3. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych

c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)

4. Do typowych incydentów bezpieczeństwa danych osobowych należą:

   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)

   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)

   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)

5. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:

   a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki

   b. inicjuje ewentualne działania dyscyplinarne

   c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu

   d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia

6. Administrator dokumentuje wystąpienie incydentu w tym okoliczności jego wystąpienia, skutki oraz podjęte działania zaradcze – patrz załącznik **Formularz rejestracji incydentu.**

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw i wolności osób, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

8. W przypadku naruszenia ochrony danych osobowych skutkującego wysokim ryzykiem naruszenia praw i wolności osób, administrator powiadamia osoby dotknięte.

6 ZABEZPIECZENIA: INSTRUKCJA ZARZĄDZANIA RODO

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik **Instrukcja zarządzania RODO**.
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

7 ZABEZPIECZENIA: REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik - **Regulamin Ochrony Danych Osobowych**.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności.

8 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą załącznika **Plan szkolenia RODO.**
4. Materiały szkoleniowe dla uczestników szkolenia opracowano w formie załącznika **Szkolenie wewnętrzne** RODO
5. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz załącznik **04a Oświadczenie poufności**.

9 AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje procedurę audytów – załącznik **Procedura audytu**.

W celu udokumentowania przeprowadzenia audytu, Administrator wykorzystuje załącznik **Audyt RODO.**

10 PLAN CIĄGŁOŚCI DZIAŁANIA

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w załączniku **Plan ciągłości działania.**