

Analiza ryzyka związanego z przetwarzaniem danych osobowych w przedsiębiorstwie Instytut Dietetyki i Promocji Zdrowia Katarzyna Kaszyca

1. Ustalenie kontekstu

1.1. Określenie informacji i uwarunkowań związanych z działaniem przedsiębiorstwa

- a. Przedsiębiorstwo prowadzone jest w formie jednoosobowej działalności gospodarczej Katarzyny Kaszyca pod firmą Instytut Dietetyki i Promocji Zdrowia Katarzyna Kaszyca (dalej także: „Instytut”). Adres głównego miejsca wykonywania działalności: ul. Kosztowska 27, 41-409 Mysłowice. Działalność wykonywana jest także w Tychach (ul. Owczarska 9, 43-100) oraz w ograniczonym wymiarze czasowym w Katowicach (ul. Podgórna 4/4, 40-955 Katowice) oraz Zabrze (ul. Wolności 338b, 41-800 Zabrze).
- b. Głównym przedmiotem działalności przedsiębiorstwa jest przygotowywanie kompleksowych programów diet. Z uwagi na taką specyfikę działalności, klientami Instytutu są niemal wyłącznie osoby fizyczne, zawierające z Instytutem umowy w zakresie niezwiązanym z ich działalnością gospodarczą lub zawodową.
- c. Przedsiębiorstwo zatrudnia ... osób, rotacja pracowników jest stosunkowo niewielka. Większość zatrudnionych stanowią dietetycy, których zadaniem jest przeprowadzenie z klientami wywiadu i ustalenie odpowiedniej diety na podstawie takiego wywiadu oraz ewentualnie wyników badań medycznych. Dietetycy najczęściej sporządzają programy diet indywidualnie, konsultując je z właścicielką firmy, dietetykiem Katarzyną Kaszycą. Decyzję o przydzieleniu danym pracownikom konkretnego zadania ustalenia diety podejmuje właścicielka firmy, Katarzyna Kaszyca. Oprócz dietetyków, w firmie zatrudnione są osoby zapewniające obsługę administracyjną w biurze w Tychach przy ul. Owczarskiej 9.
- d. Firma korzysta z pomocy osób trzecich przy wykonywaniu umów zawartych z klientami:
 - w zakresie transportu próbek włosów, krwi z palca, wymazu z policzka do laboratoriów przeprowadzających odpowiednie badania
 - w zakresie przeprowadzania badań w/w próbek - z laboratoriami
 - w zakresie wydawania programów diety w formie papierowej poza placówką w Tychach - z recepcjonistkami zapewniającymi obsługę administracyjną zlokalizowanych tam biur
- e. Przedsiębiorstwo współpracuje ponadto ściśle z biurem księgowym (odpowiadającym także od strony formalnej za kwestie kadrowe)
- f. Przedsiębiorstwo posiada swoją stronę internetową: <https://instytutdietetyki.pl>. Strona zawiera informacje o prowadzonej działalności, dane kontaktowe do Instytutu, referencje od klientów, informacje o partnerach biznesowych, formularz kontaktowy, ponadto strona umożliwia zapisanie się na szkolenia prowadzone przez Instytut oraz zgłoszenie się do otrzymywania newslettera. Strona prowadzona jest przez pracownika Instytutu, który odpowiada równocześnie za poprawne funkcjonowanie sprzętu elektronicznego wykorzystywanego w firmie.
- g. Działalność związana z obsługą klientów prowadzona jest w przeważającej mierze w biurze mieszczącym się w Tychach przy ul. Owczarskiej 9. Biuro mieści się w części samodzielnego budynku zlokalizowanego w otoczeniu budynków jednorodzinnych. Pracownicy praktycznie nie wykonują swoich obowiązków poza biurem w Tychach oraz pomieszczeniami wynajmowanymi w Katowicach i Zabrzu podczas godzin przyjęć klientów.

Sporządzane programy diet wydawane są klientom w biurze w Tychach lub w Katowicach i Zabrze, a także, w części przypadków, w wersji elektronicznej przesyłane na adres e-mail klienta. Niektóre szkolenia oferowane przez firmę prowadzone są na odległość, za pośrednictwem Internetu, zaś materiały szkoleniowe i dyplomy poświadczające ukończenie kursu wysyłane są wówczas pocztą lub kurierem.

1.2. Opis aktywów, przetwarzanych danych i ich klasyfikacja

a. Aktywa przedsiębiorstwa, które wiążą się z przetwarzaniem danych osobowych:

- o sprzęt: ... komputery, serwery, niszczarka etc.
- o oprogramowanie: ...
- o sieć ...
- o personel - dietetycy..., administracja..., ...
- o biuro i jego wyposażenie (z wyłączeniem sprzętu wskazanego wyżej): ... budynek wolnostojący, segregatory, zamykane szafy, sejf, drzwi przeciwłamaniowe, gaśnice, monitoring...

b. Przetwarzane dane osobowe w odniesieniu do kategorii osób, których dane dotyczą:

I. klienci Instytutu (zamawiający dietę; zamawiający za pośrednictwem Instytutu badania włosów, krwi z palca, wymazu z policzka; uczestnicy szkoleń)

- Instytut przetwarza dane osobowe klientów będących osobami fizycznymi.
- Dane w/w osób przetwarzane przez Konspekt obejmują (maksymalnie): imię, nazwisko, adres e-mail, numeru telefonu, adres do korespondencji, adres zamieszkania, numer PESEL, data urodzenia, płeć, miejsce urodzenia, numer i seria dowodu osobistego. Do sporządzenia diety dane osobowe zbierane podczas wywiadu z dietetykiem obejmują dodatkowo: wagę, wzrost, ciśnienie, informacje dotyczące przemiany materii przez organizm klienta, trybie życia klienta (kaloryczność dotychczasowej diety, godziny posiłków, nawyki żywieniowe, aktywność fizyczna), a w części przypadków także inne dane dotyczące zdrowia - informacje o przebytych lub trwających chorobach, zabiegach medycznych, wynikach badań medycznych, nietolerancji pokarmowej, alergiach. Jako podmiot pośredniczący / zlecający badania w zewnętrznych laboratoriach, na życzenie klienta, Instytut pobiera od niego próbki włosów, krwi z palca, wymaz z policzka oraz dane niezbędne do wykonania badania wymagane przez te zewnętrzne laboratoria.
- Dane w/w osób przetwarzane są w celu zawarcia lub zmiany umowy, należytego jej wykonania, realizowania uprawnień z tytułu rękojmi / gwarancji, dochodzenia roszczeń wynikających z umowy.
- Dane w/w osób (w zakresie imienia, nazwiska, adresu e-mail, numeru telefonu, adresu do korespondencji) mogą być wykorzystywane także do marketingu bezpośredniego przez Instytut z racji pozostawania z tymi osobami w relacji biznesowej.
- Dane w/w osób przetwarzane są przez administratora (Instytut), a w jego imieniu przez jego pracowników zaangażowanych przez administratora w realizację umowy lub wykonujących zadania z zakresu marketingu bezpośredniego. W niezbędnym zakresie, dane w/w osób przetwarzane są przez zewnętrzne laboratoria (tj. podmioty wykonujące na życzenie klientów badania w w/w zakresie).

II. potencjalni klienci Instytutu (osoby kontaktujące się z Instytutem z zamiarem zawarcia umowy z zakresu działalności Instytutu)

- Konspekt przetwarza dane osobowe potencjalnych klientów będących osobami fizycznymi. Dane w/w osób przetwarzane przez Instytut obejmują (maksymalnie): imię, nazwisko, firma, adres e-mail, numeru telefonu, adres do korespondencji; w odniesieniu zaś do przedstawicieli osób prawnych lub jednostek organizacyjnych niebędących osobami prawnymi, którym ustawa przyznaje zdolność prawną oraz podobnych podmiotów niebędących osobami fizycznymi, przetwarzane są również dane umożliwiające potwierdzenie umocowania osoby działającej w imieniu takiego podmiotu i przyporządkowanie jej do danego podmiotu w dokumentacji związanej ze złożeniem oferty i przygotowaniem umowy.
- Dane w/w osób przetwarzane są w celu wykonania czynności mających na celu zawarcie umowy (np. złożenie oferty, negocjacja warunków umowy), ewentualnie dochodzenia roszczeń, jeżeli takie ujawniły się już na etapie negocjacji.
- Dane w/w osób (w zakresie imienia, nazwiska, adresu e-mail, numeru telefonu, adresu do korespondencji) mogą być wykorzystywane także do marketingu bezpośredniego przez Konspekt jeżeli osoby, których dane dotyczą wyrażą na to zgodę.
- Dane w/w osób przetwarzane są przez administratora, a w jego imieniu przez jego pracowników zaangażowanych przez administratora do prowadzenia negocjacji i podejmowania innych czynności zmierzających do zawarcia umowy z potencjalnym klientem, a także, jeżeli ma to zastosowanie, wykonujących zadania z zakresu marketingu bezpośredniego. Jeżeli administrator do negocjacji, przygotowania umowy lub marketingu bezpośredniego angażuje przedstawiciela handlowego, również on przetwarza dane osobowe w/w osób.

III. pracownicy Instytutu

- Instytut przetwarza dane osobowe pracowników.
- Dane w/w osób przetwarzane przez Instytut obejmują dane niezbędne do wywiązywania się przez Konspekt z obowiązków wynikających z obowiązującego prawa (w szczególności Kodeksu pracy), oraz przekazywane przez pracowników dobrowolnie (wówczas przetwarzane są na podstawie zgody, np. jeśli chodzi o zdjęcie pracownika). Dane te mogą obejmować w szczególności: imię, nazwisko, adres e-mail, numeru telefonu, adres do korespondencji, adres zamieszkania, numer PESEL, numer dowodu osobistego lub paszportu, datę wydania i ważności dowodu osobistego lub paszportu, organ wydający dowód osobisty lub paszport, dane dotyczące kwalifikacji zawodowych, dane dotyczące wykorzystanego urlopu i innych dni wolnych, dane dotyczące jakości pracy, dane pochodzące z ewidencji czasu pracy, dane dotyczące wynagrodzenia, zwolnień lekarskich.
- Dane w/w osób przetwarzane są w celu wywiązania się przez Instytut z obowiązków nałożonych przez prawo pracy i prawo ubezpieczeń społecznych, a także w celu realizacji uzasadnionego interesu administratora polegającego na efektywnym zarządzaniu przedsiębiorstwem, odpowiednim wykorzystaniu personelu, przestrzeganiu dyscypliny pracy oraz w celu dochodzenia roszczeń wynikających z umowy o pracę.
- Dane w/w osób przetwarzane są przez administratora, a w jego imieniu przez jego pracowników zaangażowanych przez administratora w realizację polityki kadrowej. W zakresie prowadzenia dokumentacji księgowej i w ograniczonym zakresie spraw kadrowych (obliczanie wynagrodzenia, urlopów, ewidencjonowanie zwolnień lekarskich, obliczanie składek na ubezpieczenie społeczne itp.) przetwarza je księgowa Instytutu. W ograniczonym zakresie, podyktowanym wykonywaniem przez pracowników obowiązków pracowniczych, dane osobowe pracowników przetwarzane są przez klientów, potencjalnych klientów i podwykonawców, z którymi pracownicy ci się kontaktują w związku z w/w czynnościami podejmowanymi wobec tych osób przez Instytut.
- W procesie rekrutacji przetwarzane są tylko te dane, których może żądać pracodawca na podstawie przepisów kodeksu pracy oraz te, które są istotne z punktu widzenia procesu rekrutacyjnego i zostały podane dobrowolnie przez kandydata, a przetwarzanie następuje za jego zgodą.

- Przetwarzanie danych praktykantów i stażystów odbywa się na analogicznych zasadach jak pracowników, z uwzględnieniem zakresu ich obowiązków oraz obowiązków administratora wobec tych osób.

IV. księgowość

- Instytut na podstawie umowy cywilnoprawnej przekazuje pewne dane osobowe pracowników, klientów, kontrahentów do ..., który świadczy usługi z zakresu księgowości i obsługi kadrowej.
- Dane osobowe dotyczące osoby prowadzącej księgowość przetwarzane są wyłącznie w celu realizacji zawartej z nią umowy mającej za przedmiot obsługę księgowo-kadrową Instytutu.

c. charakterystyka przetwarzanych danych osobowych

- Część danych osobowych przetwarzanych przez Instytut należy do szczególnej kategorii danych wskazanych w art. 9 RODO - są to dane dotyczące zdrowia. Ułożenie odpowiedniej diety klientowi w większości wypadków wymaga jednak poznania stanu jego zdrowia, w większości wypadków klienci sami dostarczają wyniki badań lekarskich ażeby umożliwić Instytutowi należyte wykonanie umowy, w każdym zaś wypadku przetwarzanie tego rodzaju danych odbywa się za wyraźną zgodą osoby, której dane dotyczą. Na tych samych zasadach odbywa się pośredniczenie - na życzenie klienta - w wykonaniu badań włosów, krwi z palca, wymazu z policzka, tj. klient każdorazowo daje wyraźną zgodę na pobranie danego materiału, jego wysyłkę do zewnętrznego laboratorium i, jeśli ma to zastosowanie, do przetwarzania wyników badań w celu ustalenia optymalnej diety. Pozostałe dane osobowe przetwarzane przez Instytut, czy to dane klientów (w tym uczestników szkoleń) czy potencjalnych klientów, nie zaliczają się do szczególnych kategorii danych osobowych wymienionych w art. 9 i 10 RODO - dane dotyczące zdrowia danej osoby niezbędne są dopiero na etapie opracowywania diety, a więc w wykonaniu zawartej z klientem umowy mającej za przedmiot właśnie usługę polegającą na konsultacji z dietetykiem i ułożeniem diety.
- Instytut przetwarza dane osobowe pracowników, które w pewnym zakresie należą do szczególnych kategorii danych osobowych, a to danych dotyczących zdrowia. Przetwarzanie tego typu danych jest jednak niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, zgodnie z polskim prawem.
- W przeważającej większości dane przetwarzane przez Instytut to dane, których przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. W części wypadków przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (jak wyżej wskazano, zaliczyć tutaj należy marketing bezpośredni w stosunku do klientów, kontrolowanie jakości pracy lub świadczonych na rzecz Instytutu usług celem efektywnego zarządzania przedsiębiorstwem).
- Co do danych pracowników, codziennie podpisują oni listę obecności; dane dotyczące urlopów, zwolnień lekarskich, wynagrodzenia itp. wykorzystywane są przez administratora i upoważnione przez niego osoby (upoważnieni pracownicy, księgowa) rzadziej, zgodnie z bieżącym zapotrzebowaniem. Nie stosuje się w miejscu pracy takich metod identyfikowania i kontrolowania pracowników jak: monitoring (budynek przy Owczarskiej 9 w Tychach objęty jest monitoringiem, jednak nie jest wykorzystywany dla celów ewidencji czasu pracy ani identyfikacji pracowników, a ma na celu zabezpieczenie obiektu jako całości), elektroniczna rejestracja czasu pracy, oprogramowanie służące do śledzenia czasu pracy przy komputerze, śledzenie lokalizacji służbowych samochodów lub sprzętu elektronicznego itp.

1.3. Szczegółowy opis stosowanych zabezpieczeń i innych ograniczeń

Instytut stosuje następujące zabezpieczenia mające wpływ na ochronę przetwarzanych danych osobowych:

A. Zabezpieczenia organizacyjne

- (1) Wprowadzenie „Polityki bezpieczeństwa przetwarzania danych osobowych”
- (2) Wprowadzenie „Instrukcji postępowania w przypadku naruszenia ochrony danych”
- (3) Organizowanie szkoleń z zakresu ochrony danych osobowych dla pracowników, w szczególności w razie zmian prawnych lub zmian wewnętrznych polityk obowiązujących w przedsiębiorstwie
- (4) Prowadzenie rejestru naruszeń ochrony danych osobowych
- (5) Okresowe przeglądy stosowanych zabezpieczeń i dostosowywanie poziomu zabezpieczeń do zmieniających się zagrożeń i związanego z nimi ryzyka wystąpienia naruszeń ochrony danych osobowych
- (6) Wprowadzenie klauzul informacyjnych skierowanych do osób, których przetwarzane dane dotyczą
- (7) Prowadzenie rejestru czynności przetwarzania danych osobowych

B. Zabezpieczenia personalne

- (8) Zawarcie umów z podmiotami przetwarzającymi dane osobowe w imieniu administratora
- (9) Wprowadzenie upoważnień dla pracowników do przetwarzania danych osobowych, z zastosowaniem ograniczenia dostępu niektórych pracowników do niektórych danych
- (10) Prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych w przedsiębiorstwie administratora, ze wskazaniem zakresu takiego przetwarzania
- (11) Wprowadzenie postanowień umownych w zakresie zobowiązania do zachowania poufności

C. Zabezpieczenia techniczne

- (12) Na komputerach służących do pracy zainstalowano oprogramowanie antywirusowe ..., aktywny jest firewall
- (13) Tworzenie kopii zapasowych przechowywanych w innym miejscu
- (14) Dostęp do określonych danych chroniony jest hasłem
- (15) Przenośne nośniki danych (np. pendrive, płyta CD) są szyfrowane
- (16) Dostęp do poczty elektronicznej chroniony jest hasłem
- (17) Przenośne urządzenia elektroniczne (laptopy, telefony), chronione są hasłem, kodem PIN

D. Zabezpieczenia fizyczne

- (18)Zabezpieczenie fizyczne budynków wykorzystywanych jako biura oraz gabinety dietetyków: do części budynku wydzielonej pod prowadzenie działalności przez Instytut a także do poszczególnych pomieszczeń biurowych (gabinetów dietetyków) prowadzą drzwi zamykane na klucz, teren wokół budynku oraz w części wspólnej budynku jest monitorowany, zainstalowano system alarmowy, ochronę budynku zapewnia wyspecjalizowana firma zewnętrzna;
- (19)Zabezpieczenie fizyczne wyposażenia biurowego: dane osobowe utrwalone na nośnikach tradycyjnych (papierowe) przechowywane są w zamykanych szafach / szufladach lub sejfie, a ich kopie zapasowe w innym miejscu,
- (20)W związku z zagrożeniami żywiołami: funkcjonuje system przeciwpożarowy, budynek wyposażony jest w gaśnice, piorunochron
- (21)Nośniki zawierające dane osobowe, po ustaniu ich przydatności, niszczone są z użyciem niszczarek uniemożliwiających odtworzenie nośnika bądź wszelkie dane są z nich trwale usuwane (dotyczy nośników elektronicznych).

1.4 .Określenie kryteriów akceptacji ryzyka

W ramach niniejszego opracowania poziom ryzyka zostanie wyznaczony przez iloczyn współczynnika skutku i prawdopodobieństwa jego wystąpienia (oba współczynniki będą określone w przedziale od 1 do 5) - zob. pkt 2 opracowania.

W ten sposób poziom ryzyka zostanie określony jako:

1. **niski (iloczyn 1-3)**
2. **średni (iloczyn 4-6)**
3. **wysoki (iloczyn 8-12)**
4. **krytyczny (iloczyn 15 lub wyższy)**

Akceptowany przez administratora poziom ryzyka to poziom niski.

Sklasyfikowanie ryzyka na poziomie „niski” oznacza, że podejmowanie działań w celu zmniejszenia ryzyka nie jest niezbędne, jednak konieczne pozostaje stałe monitorowanie i kontrola procesów przetwarzania danych osobowych, ażeby móc wychwycić zwiększenie się ryzyka. Poziom krytyczny jest poziomem nietolerowanym i wymaga natychmiastowego działania ze strony administratora. Co do poziomów średniego i wysokiego, oznacza on konieczność podjęcia przez administratora działań celem zmniejszenia ryzyka, lecz nie muszą być one podjęte natychmiast - można odłożyć je w czasie, przy czym im wyższy iloczyn, tym ten czas powinien być krótszy.

2. Mechanizmy kontrolne

W tym punkcie opracowania zostanie dokonana identyfikacja wymagań dla procesów przetwarzania danych w kontekście celów działalności administratora, a następnie stwierdzone zostanie czy wymagania są wypełniane.

Wymogi co do zasad i podstaw prawnych przetwarzania danych osobowych.

Podstawa prawna RODO (artykuł)	Zasada przetwarzania danych osobowych / podstawa prawna przetwarzania /	Uwagi i pytania pomocnicze	Ocena wypełniania wymogu (tak / nie / nie dotyczy)
art. 5 ust. 1 lit. a	Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”); Podstawy przetwarzania danych osobowych:	Przetwarzanie danych osobowych musi być oparte przynajmniej na jednej z niżej wymienionych przesłanek by było zgodne z prawem (legalność), przetwarzając należy mieć na uwadze obowiązujące przepisy i interesy osoby, której dane dotyczą (rzetelność), a wszelkie związane z przetwarzaniem danych komunikaty adresowane do osób, których dane dotyczą, powinny być dla nich zrozumiałe i łatwo dostępne.	
Art. 6 ust. 1 lit. a	osoba, której dane dotyczą wyraziła zgode na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;	Zgoda 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. • Czy jeśli nie ma zastosowania inna z poniższych przesłanek przetwarzania danych osobowych, administrator jest pewny, że zgodę taką uzyskał? • Czy jeśli podstawa do przetwarzania danych osobowych pracownika nie mieści się w innych przesłankach, administrator uzyskał zgodę pracownika do przetwarzania jego danych (dotyczy np. umieszczenia zdjęcia na stronie internetowej)? • Czy klauzula zgody zawiera określenie celów przetwarzania? • Czy można odtworzyć treść udzielonych zgód w stosunku do konkretnej osoby, która ich udzieliła?	
Art. 6 ust. 1 lit. b	przetwarzanie jest niezbędne do wykonania umowy , której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;	Dotyczy wykonywania umów z klientami oraz czynności dokonywanych w stosunku do potencjalnych klientów.	

Art. 6 ust. 1 lit. c	przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;	Dotyczy stosunku pracy (obowiązki prawne ustalone zostały m.in. w ustawach: kodeks pracy, w wypadku cudzoziemców wymogi ustawy o cudzoziemcach, ustawy o promocji zatrudnienia i instytucjach rynku pracy), wymogów co do zawartości projektu (zgodnie z Prawem budowlanym). Należy umieć wskazać podstawę prawną takiego obowiązku.	
Art. 6 ust. 1 lit. d	przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;	Dotyczyć może tylko wyjątkowych sytuacji, gdy dana osoba nie jest w stanie wyrazić zgody samodzielnie (np. w związku z chorobą) a przetwarzanie jej danych jest niezbędne by chronić jej żywotne interesy takie jak zdrowie czy życie.	
Art. 6 ust. 1 lit. e	przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi		
Art. 6 ust. 1 lit. f	przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.	Dotyczy w szczególności marketingu bezpośredniego kierowanego do klientów oraz podobnych sytuacji, w których administrator może przyjąć, że jego uzasadniony interes (który potrafi wskazać) w danych okolicznościach przeważa (jest obiektywnie istotniejszy) niż interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych.	
art. 5 ust. 1 lit. b	Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; („ograniczenie celu”)	Czy dane są przetwarzane tylko w takim celu, w jakim były zbierane (np. nie dochodzi do sytuacji, w której klient zawierający umowę mającą za przedmiot ułożenie diety i w związku z zawartą z nim umową przetwarzano jego dane osobowe, otrzymuje później na swój numer telefonu oferty dotyczące szkoleń, chociaż co do takich usług nigdy nie wyrażał zainteresowania)?	
art. 5 ust. 1 lit. c	adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);	Czy Instytut nie wymaga od osób fizycznych danych, które obiektywnie nie są mu potrzebne do celu, dla którego dane przetwarza (np. podczas negocjacji z potencjalnym klientem wymagane są od niego informacje o jego stanie zdrowia)?	
art. 5 ust. 1 lit. d	Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);	Czy podejmuje się działania mające na celu doprowadzenia do merytorycznej poprawności przetwarzanych danych osobowych?	

art. 5 ust. 1 lit. e	Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; („ograniczenie przechowywania”);	Czy po upływie okresu, kiedy przetwarzanie (w tym przechowywanie) danych osobowych było uzasadnione, dane osobowe są anonimizowane lub usuwane?	
art. 5 ust. 1 lit. f	Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).	- Czy sprawdzane są okresowo zabezpieczenia stosowane w przedsiębiorstwie a związane z ochroną danych osobowych? - Czy stosowane są odpowiednie środki techniczne i organizacyjne zwiększające bezpieczeństwo przetwarzania danych osobowych?	
art. 5 ust. 2	Administrator jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).	- Czy administrator ma bieżącą kontrolę nad przetwarzaniem danych osobowych? - Czy wątpliwości w zakresie ochrony danych osobowych są mu zgłaszane przez pracowników? - Czy przypadki naruszeń ochrony danych osobowych są administratorowi zgłaszane przez pracowników lub podmioty współpracujące z administratorem? - Czy prowadzona jest dokumentacja, która w razie potrzeby, w szczególności w razie kontroli organu nadzorczego, pozwoli administratorowi na wykazanie, że powyższych zasad rzeczywiście przestrzega?	

Wymogi co do wypełniania obowiązków informacyjnych względem osób, których dane dotyczą

Podstawa prawna RODO (artykuł)	Zakres obowiązku informacyjnego	Uwagi i pytania pomocnicze	Ocena wypełniania wymogu (tak / nie / nie dotyczy)
--------------------------------	---------------------------------	----------------------------	--

Art. 13 ust. 1	Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje: a) swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych osobowych oraz podstawę prawną przetwarzania; c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania; d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.	W celu spełnienia obowiązku informacyjnego należy poinformować osobę, której dane dotyczą o: - nazwie administratora danych, adresie i danych kontaktowych, - danych kontaktowych inspektora ochrony danych osobowych, - celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania (np. zgoda, przepis prawa), - jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f (do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią) - należy poinformować o prawnie uzasadnionych interesach realizowanych przez administratora, - odbiorcach danych lub kategoriach odbiorców danych, jeżeli istnieją, - gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, - okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu, - prawie żądania od administratora dostępu do danych osobowych osoby, której dane dotyczą, - prawie do cofnięcia zgody w dowolnym momencie (cofnięcie zgody w przypadku studentów odbywających tok studiów cofnięcie zgody nie jest możliwe, z uwagi na to, że dane przetwarzane są na podstawie przepisów prawa), - prawie wniesienia skargi do organu nadzorczego, - obowiązku ustawowym lub umownym lub warunku zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ew. konsekwencje niepodania danych, - (gdy ma to zastosowanie) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu. W przypadku zbierania danych nie od osoby, której dane dotyczą (art. 14 ust.	
-----------------------	--	--	--

Art. 13 ust. 2	Poza powyższymi informacjami, podczas pozyskiwania danych osobowych administrator podaje osobie, której one dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania: a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu; b) informacje o prawie żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d) informacje o prawie wniesienia skargi do organu nadzorczego; e) informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych; f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.	w przypadku zbierania danych, nie od osoby, której dane dotyczą (art. 14 ust. 2 lit. f), należy poinformować tę osobę dodatkowo o: - źródle pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych. Obowiązek informacyjny należy spełnić przed rozpoczęciem zbierania danych osobowych. Obowiązek informacyjny można spełnić przez wprowadzenie tzw. klauzul informacyjnych. Klauzula informacyjna może przyjąć postać informacji: - zamieszczonej w formularzu, - zamieszczonej w regulaminie, - zamieszczonej w mailu, - zamieszczonej na stronie internetowej. • Czy jednostka organizacyjna wykonuje obowiązek informacyjny? • Czy klauzule informacyjne są zgodne z przepisami RODO? • Czy obowiązek informacyjny jest spełniany przed rozpoczęciem przetwarzania danych osobowych?	
-----------------------	---	--	--

Wymogi co do bezpieczeństwa danych osobowych

Podstawa prawna RODO (artykuł)	Środki konieczne do zabezpieczenia przetwarzanych danych osobowych.	Uwagi i pytania pomocnicze	Ocena wypełniania wymogu (tak / nie / nie dotyczy)
---	--	----------------------------	--

Art. 32	Administrator i podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. W tym między innymi w stosownym przypadku wprowadzają: a) pseudonimizację i szyfrowanie danych osobowych; b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.	1. Czy pracownicy zostali zapoznani z Polityką bezpieczeństwa ochrony danych osobowych? 2. Czy pracownicy zostali zapoznani z Instrukcją postępowania w razie naruszenia ochrony danych osobowych? 3. Czy pracownicy mają upoważnienia do przetwarzania danych osobowych? 4. Czy pracownicy zachowują ostrożność wykorzystując nośniki, na których utrwalone są dane osobowe, zwłaszcza przy przekazywaniu danych osobowych poza przedsiębiorstwo? 5. Czy pozwala się by w miejscach gdzie przetwarzane są dane osobowe, przybywały osoby nieuprawnione bez nadzoru pracowników? 6. Czy pracownicy niszczą dokumenty papierowe zawierające dane osobowe przy użyciu niszczarki? 7. Czy z nośników elektronicznych nieodwracalnie kasuje się dane gdy przestają być niezbędne? 8. Czy przenosząc dane na nośnikach elektronicznych szyfruje się ich zawartość? 9. Czy ograniczono dostęp do programów / urządzeń, w których przetwarza się dane osobowe przez zastosowanie logowania z użyciem hasła? 10. Czy pracownicy są świadomi obowiązku zgłaszania przypadków naruszenia ochrony danych osobowych? 11. Czy pracownicy wiedzą, że dokumenty papierowe należy przenosić w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby postronne? 12. Czy pracownicy zostali zaznajomieni z przepisami regulującymi ochronę danych osobowych? 13. Czy dane osobowe zabezpieczone są w sposób fizyczny? 14. Czy kopie zapasowe lub archiwalne, zawierające dane osobowe przechowywane są bezpiecznie, w odrębnym pomieszczeniu? 15. Czy przestrzeń biurowa zabezpieczona jest przed dostępem osób nieuprawnionych? 16. Czy użyto Firewall do ochrony dostępu do sieci komputerowej? 17. Czy używane są programy antywirusowe? 18. Czy nośniki informacji podłączone do stacji roboczej sprawdzane są oprogramowaniem antywirusowym? 19. Czy systemy operacyjne i przeglądarki mają instalowane aktualizacje? 20. Czy stosuje się wygaszacze ekranów? 21. Czy ekrany monitorów zostały ustawione w sposób uniemożliwiający wgląd przez osoby nieuprawnione odwiedzające biuro?	
-----------------------	---	--	--

3. Szacowanie ryzyka

W ramach szacowania ryzyka, dla każdego scenariusza urzeczywistnienia się zidentyfikowanych zagrożeń, wykonywana jest ocena prawdopodobieństwa jego zajścia oraz szacowanie skutków jego zmaterializowania się. Po wyznaczeniu prawdopodobieństwa wystąpienia określonego zdarzenia oraz strat, jakie mogą być nim spowodowane (tj. wielkość skutku), możliwe będzie wyznaczenie wartości ryzyka (oznaczone literą „R”) jako iloczynu prawdopodobieństwa wystąpienia danego zdarzenia (oznaczone literą „P”) i jego skutku (oznaczony literą „S”) [zob. tabela poniżej].

Wyznaczenie wartości skutku w skali od 1 do 5

Skutek	Poziom	Opis skutku	
		W aspekcie materialnym (finansowym)	W aspekcie niematerialnym (wpływu na reputację, stworzenia zagrożenia dla interesów innych osób, ponoszenia odpowiedzialności administracyjnej lub karnej)
Bardzo wysoki	5	powyżej 1 mln zł	Mogą pojawić się negatywne opinie w mediach międzynarodowych. Naruszenie może doprowadzić do poważnego naruszenia interesów osób trzecich i ich roszczeń odszkodowawczych, odpowiedzialności karnej osób odpowiedzialnych za ochronę informacji. Mogą wystąpić daleko idące, w tym nieodwracalne konsekwencje, których osoby nie są w stanie pokonać (np. znaczne trudności finansowe, niezdolność do pracy, długoterminowe dolegliwości psychiczne lub fizyczne, śmierć)
Wysoki	4	w zakresie 500 tys. - 1 mln zł	Mogą pojawić się negatywne opinie w mediach krajowych. Naruszenie dotyczy informacji o charakterze wrażliwym, jednak nie powinno wiązać się z odpowiedzialnością karną osób odpowiedzialnych za ochronę informacji, może wiązać się z odpowiedzialnością administracyjną. Mogą wystąpić istotne konsekwencje, które powinno udać się pokonać ale ze znacznymi trudnościami (np. sprzeniewierzenie funduszy, uszkodzenie mienia, utrata pracy, spór sądowy, negatywny wpływ na stan zdrowia).
Średni	3	w zakresie 100 - 500 tys. zł	Mogą pojawić się negatywne opinie w mediach lokalnych. Naruszenie dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, jednak nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za ochronę informacji. Mogą wystąpić pewne niedogodności, które osoby będą zdolne przezwyciężyć pomimo trudności (np. dodatkowe koszty, stres).
Niski	2	w zakresie 5 - 100 tys. zł	Mogą pojawić się negatywne opinie, jednak bez udziału mediów. Naruszenie dotyczy spraw mniejszej wagi, odnosi się do pojedynczych przypadków i nie wiąże się odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za ochronę informacji. Osoby fizyczne nie będą dotknięte konsekwencjami, ewentualnie napotkać mogą jedynie niedogodności i drobne utrudnienia, które z łatwością pokonają (np. konieczność ponownego wprowadzenia danych).
Bardzo niski	1	poniżej 5 tys. zł	Obejmuje sytuacje, gdy skutek nie występuje, ewentualnie nie ma wpływu bądź ma marginalny wpływ na reputację (ewentualnie nie będzie zauważalnych skutków), konsekwencje praktycznie nie obejmują odczuwalnych dolegliwości dla osób, których naruszenie może dotyczyć. Praktycznie brak wpływu na funkcjonowanie procesu przetwarzania danych.

Wyznaczenie wartości prawdopodobieństwa wystąpienia skutku w skali od 1 do 5 (przy ocenie należy brać pod uwagę w szczególności: statystyki dotyczące podobnych zdarzeń, atrakcyjność aktywu, istniejące zabezpieczenia)

Prawdopodobieństwo	Poziom	Opis
Prawie pewne	5	zdarzenie występuje co najmniej raz w tygodniu
Prawdopodobne	4	zdarzenie występuje co najmniej raz w miesiącu
Możliwe	3	zdarzenie występuje co najmniej raz na kwartał
Mało prawdopodobne	2	zdarzenie występuje co najmniej raz na pół roku
Rzadkie	1	zdarzenie nie występuje lub występuje raz w roku

L.p.	Zagrożenia dla bezpieczeństwa danych osobowych →	Kradzież			Pozostawienie bez nadzoru			Uzyskanie dostępu przez osobę nieuprawnioną			Utrata przez zagubienie			Utrata przez działanie sił przyrody (ogień, woda)			Awaria sprzętu			Zniszczenie			Brak personelu kompetentnego w danym zakresie			Wadliwe wprowadzenie danych			Atak z użyciem złośliwego oprogramowania			Próba wyłudzenia danych		
	Aktywa / czynności przetwarzania / procesy biznesowe narażone na wskazane zagrożenia ↓	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R	S	P	R			
1	Komputery stacjonarne																																	
2	Komputery przenośne																																	
3	Urządzenia mobilne (smartfony, tablety, itp.)																																	
4	Elektroniczne nośniki informacji (dyski, pendrive, płyty CD)																																	

Ryzyko pozostaje na akceptowalnym poziomie, na chwilę obecną nie jest konieczne podjęcie czynności mających na celu obniżenie ryzyka. Niezbędne jest natomiast bieżące monitorowanie poziomu ryzyka.

5. Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Zgodnie z art. 35 RODO, jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:

- a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub
- c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Dalej, zgodnie z art. 36 RODO, jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

W związku z faktem, że Instytut przetwarza dane osobowe należące do szczególnych kategorii, o których mowa w art. 9 ust. 1 (dane dotyczące zdrowia), poddano analizie, czy w związku z tym nie spełnia przesłanki dokonania oceny skutków dla ochrony danych w szczególności z uwzględnieniem brzmienia art. 35 ust. 3 lit. b) RODO, tj. czy dane te nie są przetwarzane na dużą skalę. Tak dokonana analiza posłużyła również do stwierdzenia czy w myśl art. 37 ust. 1 lit. c) RODO nie jest wymagane powołanie inspektora ochrony danych (w myśl tego przepisu powołanie takie jest konieczne gdy główna działalność administratora polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych). Ustalenie zatem czy w Instytucie dane dotyczące zdrowia przetwarzane są na dużą skalę, umożliwia odpowiedź na pytanie zarówno o konieczność przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (art. 35 RODO), jak i o konieczność powołania inspektora ochrony danych (art. 37 RODO).

Co tyczy się przetwarzania danych na dużą skalę, zauważyć należy, że RODO nie zawiera żadnych konkretnych wskazówek ilościowych w tym zakresie. Oceniając sytuację Instytutu, należało zważyć, że:

- a. w trakcie prac legislacyjnych nad RODO w Parlamencie Europejskim zaproponowano, aby jedną z przesłanek wyznaczenia inspektora było przetwarzanie danych dotyczących co najmniej 5000 osób średniorocznie. Jednak w ostatecznym tekście nie wskazano konkretnego progu (tak wskazuje się w literaturze: P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, 2018, Legalis).
- b. motyw 91 RODO mówi o „operacjach przetwarzania o dużej skali” dookreślając je jako służące „przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą”

- c. ten sam motyw RODO wskazuje, że przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa.
- d. Grupa Robocza Art. 29 jako przykład przetwarzania danych, będących główną działalnością podmiotu, dokonywaną na dużą skalę podawała w swoich opracowaniach przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności.
- e. Dalej Grupa Robocza Art. 29 rekomendowała by dla oceny skali brać pod uwagę następujące czynniki: 1) liczba osób, których dane są przetwarzane jako konkretną ilość lub stosunek do właściwej populacji, 2) wolumen (ilość) danych i/lub zakres różnych rodzajów danych, 3) okres przetwarzania lub stałość działalności w zakresie przetwarzania danych, 4) zakres geograficzny działalności w zakresie przetwarzania danych.

Biorąc więc pod uwagę, że:

- Instytut prowadzony jest w formie jednoosobowej działalności gospodarczej,
- średniorocznie przetwarzane są dane dotyczące około ... osób,
- w motywach RODO wprost odwołano się do działalności lekarzy i prawników, do których to skala działalności dietetyka jest porównywalna, również jeśli chodzi o zaangażowanie personelu pomocniczego
- jako przykład przetwarzania danych na dużą skalę podaje się szpital, a przetwarzanie danych w Instytucie w porównaniu do ich przetwarzania w jakimkolwiek szpitalu określić należałoby jako znikome (zdecydowanie poniżej 1% w stosunku do szpitala)

należy dojść do wniosku, że Instytut nie spełnia przesłanek obligatoryjnego przeprowadzenia oceny, o której mowa w art. 35 RODO, jak również nie spełnia przesłanek obligatoryjnego powołania inspektora danych osobowych. Z uwagi na powyższe, od przeprowadzenia w/w oceny, jak i powołania inspektora ochrony danych odstąpiono.

Na tym analizę zakończono.

Sporządzono w Tychach, ... 2018 roku

Podpis: