Dla zainteresowanych zamieszczamy poniżej pełną analizę:

Artykuł 37 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych)(dalej: RODO) stanowi: *„Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy: **główna działalność** administratora lub podmiotu przetwarzającego polega na przetwarzaniu na **dużą skalę** szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1,(...)”* Dane przetwarzane w trakcie udzielania świadczeń i w związku z ich udzielaniem, w szczególności zawarte w dokumentacji medyczne to szczególna kategoria danych osobowych,

Motyw 97 RODO zawiera takie określenie: *„W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności.”*

Motyw 91 RODO zawiera takie określenie: *„operacji przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, (...)– oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw.”* I dalej *: „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(...)”*

Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 (https://odoserwis.pl/a/1118/wytyczne-dotyczace-inspektorow-ochrony-danych-dpo) przygotowała *„Wytyczne dotyczące inspektorów ochrony danych IODo (DPO skrót od nazwy angielskiej)przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.(16/EN, WP 243 rew. 01)”* zawierają one min. następujące zapisy:

„Dla przykładu działalnością główną szpitali będzie zapewnianie opieki medycznej. Natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna. Oznacza to, że szpitale będą miały obowiązek powołania IODo (DPO).”

- RODO nie definiuje pojęcia „dużej skali” przetwarzania danych. GR Art. 29 zaleca rozważenie następujących czynników w celu określenia, czy przetwarzanie jest przeprowadzane na dużą skalę:

- Liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa;
- Zakres przetwarzanych danych osobowych;
- Okres, przez jaki dane są przetwarzane;
- Zakres geograficzny przetwarzania danych osobowych;

Do przykładów „przetwarzania na dużą skalę” zaliczyć można:

- •Przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności;
- •Przetwarzanie danych dotyczących podróży osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem ‘kart miejskich’);
- •Przetwarzanie danych geo-lokalizacyjnych klientów w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych;
- •Przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności;
- •Przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki;
- •Przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

Przykłady przetwarzania niemieszczącego się w definicji „dużej skali”:

- **•Przetwarzanie danych pacjentów, dokonywane przez pojedynczego lekarza;**

Z powyższego wynika, że obowiązek wyznaczenia Inspektora Danych Osobowych dla przychodni poz nie jest jednoznaczny. Działalnością główną przychodni jest bycie w gotowości do udzielania świadczeń zdrowotnych i w razie potrzeby ich udzielania. Jednak działalność tego typu nie byłaby możliwa bez przetwarzania danych zawartych w dokumentacji medycznej. Jako, że z zapisu art. 37 RODO obowiązek wyznaczenia IOD’o powstaje w sytuacji spełnienia dwóch warunków kumulatywnie „*zawsze gdy: **główna działalność**(…) **na dużą skalę…”*** oznacza to, że oba wskazania i „główna działalność” i „duża skala” winny być spełnione. Przy braku któregokolwiek wskazania obowiązku ustanowienia IOD’o nie powstaje.

Gdy podmiot wyznacza IOD’o na zasadzie dobrowolności, te same wymagania będą dotyczyć jego wyznaczenia, pozycji i zadań, tak jakby to wyznaczenie było obowiązkowe.

Jeśli przyjmiemy, że zgodnie ze stanowiskiem Funduszu, kontraktem na świadczenia usług w zakresie poz i faktycznym sposobem realizowania tego kontraktu działalność przychodni poz to przede wszystkim bycie w gotowości do udzielania świadczeń i dopiero w drugiej kolejności udzielanie ich jeśli taka potrzeba zaistniej, to przetwarzanie danych osobowych zawartych w dokumentacji nie będzie główną działalności niezależnie od skali. Brak jednej z dwóch przesłanek powoduje, że nie powstaje obowiązek ustanowienia IOD’o.

Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile *„można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej”..* Pojęcie łatwości kontaktu odnosi się do zadań DPO jako punktu kontaktowego w odniesieniu do osób, których dane dotyczą, organu nadzorczego, a także wewnątrz organizacji. W celu zapewnienia możliwości łatwego kontaktu z IODo, czy to wewnętrznym czy zewnętrznym, istotne jest udostępnienie jego danych kontaktowych. DPO, przy pomocy zespołu w razie konieczności, musi być w stanie efektywnie komunikować się z osobami, których dane dotyczą i współpracować z organami nadzorczymi, których sprawa dotyczy.

IODO może być członkiem personelu administratora lub podmiotu przetwarzającego (wewnętrzny IODO) lub wykonywać zadania na podstawie umowy o świadczenie usług. Oznacza to, że IODO może być zewnętrzny, i w tym przypadku jego funkcja może być wykonywana na podstawie umowy o świadczenie usług zawieranej z osobą lub organizacją.

IODo wyznacza się na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań. Wymagany poziom wiedzy fachowej powinien być określony w zależności od przeprowadzonych operacji przetwarzania danych i ochrony wymaganej do przetwarzania danych osobowych. Na przykład, gdy proces przetwarzania danych jest szczególnie złożony lub w przypadku przetwarzania dużej ilości danych szczególnych kategorii, IODo może potrzebować wyższego poziomu wiedzy i wsparcia. Odpowiednie umiejętności i wiedza obejmują:

- wiedzę na temat krajowych i europejskich przepisów i praktyk w zakresie ochrony danych, w tym dogłębnego zrozumienia RODO;
- zrozumienie przeprowadzanych procesów przetwarzania;
- zrozumienie technologii informacyjnych i bezpieczeństwa danych;
- znajomość sektora biznesowego i organizacji;
- umiejętność promowania kultury ochrony danych w organizacji.

Zgodnie z art. 39 RODO „Inspektor ochrony danych ma następujące zadania:
-a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- d) współpraca z organem nadzorczym;
- e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
- 2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.”

Nadto inspektor danych osobowych:
- winien właściwie i niezwłocznie być włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
- winien mieć zapewnione zasoby niezbędne do wykonania zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
- inspektor ochrony danych nie może otrzymywać od administratora, instrukcji dotyczących wykonywania jego zadań. Nie jest on odwoływany ani karany przez administratora. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
- osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia
- jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego - może wykonywać

inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów
Mimo wyznaczenia inspektor ochrony danych odpowiedzialność za przestrzeganie wszelkich zasad dotyczących ochrony danych osobowych odpowiada administrator danych.