Umowy powierzenia w sektorze usług zdrowotnych

Katarzyna Korulczyk
Adwokat, Inspektor ochrony Danych, LUX MED
Pracodawcy RP

GRUPA LUXMED
Jesteśmy częścią Bupa

Administrator, procesor, podprocesor – czyli kto jest kim?

- **administrator** - (art. 4 pkt 7 RODO) osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub prawie państwa członkowskiego, to również w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczenia;

- **podmiot przetwarzający (procesor)** – (art. 4 pkt 8 RODO) osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora [podmiot przetwarzający nie staje się administratorem z chwilą przekazania danych];
  Podprocesor jest również podmiotem przetwarzającym w rozumieniu RODO, natomiast podmiotem zlecającym mu przetwarzanie danych nie jest administrator, lecz upoważniony przez administratora procesor;

administrator → **procesor** → **podprocesor**
(PWDL) (dostawca usługi) (podwykonawca dostawcy usługi)

GRUPA LUXMED
Jesteśmy częścią Bupa

Podstawy prawne przetwarzania danych przez podmiot leczniczy

Co do zasady każdy **podmiot leczniczy jest niezależnym administratorem danych osobowych**, bez względu na to, czy przetwarza dane w ramach sprawowania funkcji jednostki służby medycyny pracy czy udzielania świadczeń zdrowotnych poza tym zakresem (zarówno podmioty publiczne jak i prywatne).

Argumenty:

- ma prawny obowiązek prowadzenia dokumentacji medycznej i przechowywania jej przez określony czas
- art. 30a ust. 10 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta daje PWDL możliwość zawarcia umowy powierzenia w trybie art. 31 ust. 1 uodo
- jest upoważniony przez RODO wprost do przetwarzania szczególnej kategorii danych osobowych (posiada podstawę prawną

Podstawy prawne przetwarzania danych przez podmiot leczniczy

Podmiot leczniczy w medycynie pracy jako niezależny administrator:

Argumenty:

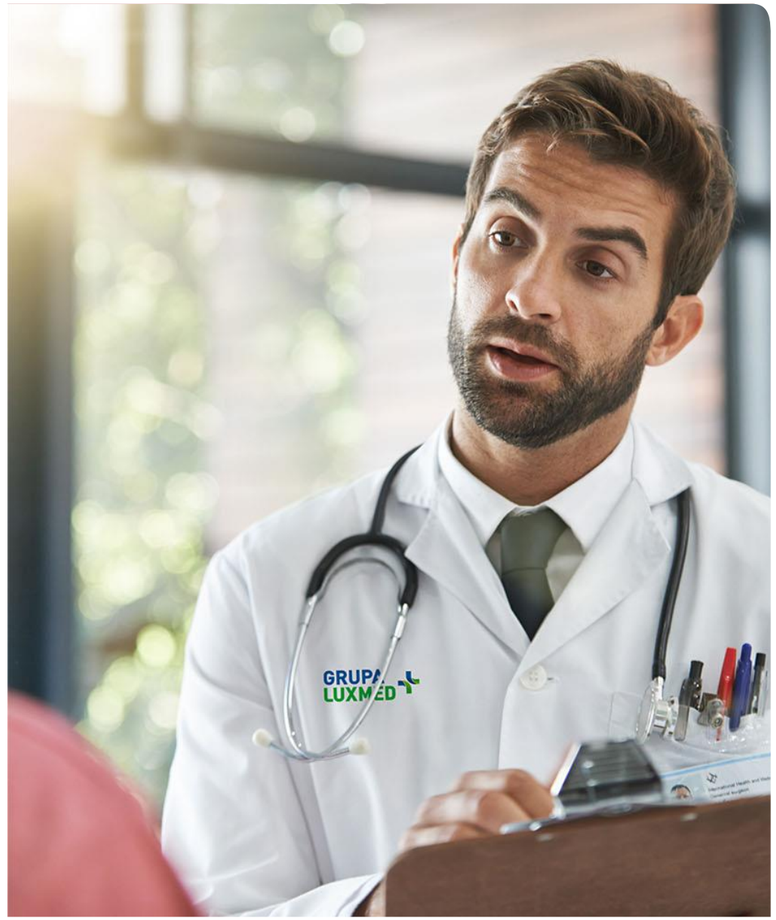
- prowadzi dokumentację medyczną
- musi zawrzeć z pracodawcą umowę o sprawowanie zadań jednostki służby medycyny pracy – ustawa o służbie medycyny pracy zawiera katalog elementów obligatoryjnych takiej umowy i brak wśród nich konieczności zawarcia powierzenia, w przeciwieństwie do art. 30a ust. 10 ustawy o prawach pacjenta i rzeczniku prac pacjenta

GRUPA LUXMED
Jesteśmy częścią Bupa

Administrator, procesor, podprocesor – czyli kto jest kim?

- Jednoosobowa praktyka lekarska nie będzie ani procesorem ani administratorem danych w przypadku, kiedy lekarz współpracuje w oparciu o kontrakt i cały ruch pacjentów jest kierowany przez kontraktujący podmiot leczniczy a jednocześnie lekarz korzysta z całego zaplecza technicznego i organizacyjnego tego podmiotu.

- W takim przypadku lekarza należy potraktować jako personel administratora i nadać mu upoważnienie do przetwarzania danych osobowych.



GRUPA LUXMED
Jesteśmy częścią Bupa

Umowa powierzenia przetwarzania danych osobowych

Ustawa z dnia 29 sierpnia 1997 r. – art. 31:

- umowa na piśmie
- określenie celu i zakresu

Od 25 maja 2018 – art. 28 RODO:

- umowa lub inny instrument prawny (odejście od wymogu pisemności)
- określenie przedmiotu, czasu przetwarzania, charakteru i celu przetwarzania, rodzaju powierzanych danych, kategorii osób, obowiązki i prawa administratora
- wskazanie obowiązków podmiotu przetwarzającego:
  - przetwarza dane na udokumentowane polecenie administratora
  - nadanie upoważnień oraz zobowiązanie personelu do zachowania danych w tajemnicy
  - zapewnienie środków bezpieczeństwa (art. 32)
  - wsparcie administratora w realizacji praw osoby, której dane dotyczą
  - wsparcie administratora w zapewnieniu bezpieczeństwa danych, identyfikacji oraz zgłaszaniu naruszeń ochrony danych, dokonywaniu skutków dla ochrony danych i ew. trybie konsultacyjnym z organem nadzoru
  - usunięcie lub zwrot danych – według decyzji administratora (po zakończeniu świadczenia usług)

Umowa powierzenia przetwarzania danych osobowych

Pozostałe obligatoryjne elementy umowy powierzenia, które mogą sprawiać trudności w ich zdefiniowaniu oraz w stosowaniu:

- określenie warunków korzystania z usług innego podmiotu przetwarzającego (podpowierzenie) – możliwe 3 modele:

  1) brak zgody
  2) zgoda szczególna (na powierzenie konkretnym podmiotom)
  3) zgoda ogólna pisemna (obowiązek powiadomienia administratora o wszystkich podprocesorach oraz ich zmianach w tym zakresie oraz umożliwienie administratorowi zgłoszenia sprzeciwu)

Warunek podpowierzenia: konieczność nałożenia umową [podpowierzenia] lub innym instrumentem prawnym na podprocesora co najmniej takich samych obowiązków, jakie zostały nałożone na procesora.

GRUPA LUXMED
Jesteśmy częścią Bupa

Umowa powierzenia przetwarzania danych osobowych

Pozostałe obligatoryjne elementy umowy powierzenia, które mogą sprawiać trudności w ich zdefiniowaniu oraz w stosowaniu:

- zobowiązanie procesora do udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków wynikających z art. 28 oraz **umożliwienie administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji;**

  Podmiot przetwarzający ma obowiązek niezwłocznego poinformowania administratora, jeżeli wydane mu polecenie w ramach uprawnień kontrolnych stanowi naruszenie RODO/przepisów Unii/państwa członkowskiego.

- Kontrola – największe wątpliwości:
  - ? zapowiedziana czy ad hoc
  - ? forma
  - ? częstotliwość
  - ? zakres kontroli
  - ? co z tajemnicą przedsiębiorstwa?
  - ? konieczność zawarcia NDA

GRUPA LUXMED
Jesteśmy częścią Bupa

Umowa powierzenia przetwarzania danych osobowych

Przekazywanie danych do państwa trzeciego (poza Unię Europejską) – czy dotyczy branży medycznej?

TAK!

Przykłady:

- przechowywanie danych w chmurze (poczta, serwery sieciowe, aplikacje)
- sprzęt diagnostyczny

GRUPA LUXMED
Jesteśmy częścią Bupa

Odpowiedzialność solidarna uczestników procesu przetwarzania danych osobowych

- art. 28 ust. 1 RODO - obowiązek korzystania przez administratora wyłącznie z usług takiego podmiotu przetwarzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniły prawa osób, których dane dotyczą

- w praktyce:
  - konieczny uprzedni oraz **udokumentowany** audyt procesora zarówno przed zawarciem umowy jak i cyklicznie, w trakcie współpracy
  - wykonanie oceny skutków dla ochrony danych oraz analiza ryzyka
  - konieczne zawarcie umowy powierzenia i określenie w niej wszystkich obowiązków stron

GRUPA LUXMED
Jesteśmy częścią Bupa

Odpowiedzialność solidarna uczestników procesu przetwarzania danych osobowych wobec podmiotu danych

Zasady odpowiedzialności określa art. 82 RODO:

- odpowiedzialność na zasadzie winy
- odpowiedzialność za szkody spowodowane przetwarzaniem naruszającym RODO ponosi administrator
- podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada na podmioty przetwarzające lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom
- jeżeli i administrator i procesor uczestniczą w tym samym przetwarzaniu i odpowiadają za szkodę spowodowaną przetwarzaniem, ich odpowiedzialność (za całą szkodę) jest solidarna

  Z powyższej odpowiedzialności administrator/procesor mogą się zwolnić, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

- prawo regresu

GRUPA LUXMED
Jesteśmy częścią Bupa

Dziękuję za uwagę

e-mail:katarzyna.korulczyk@luxmed.pl

telefon: +48 885 615 007

GRUPA LUXMED

Jesteśmy częścią Bupa