Załącznik nr 10

Wzór kwestionariusza, który dołącza się do wniosku, o którym mowa w załączniku nr 8 lub załączniku nr 9

Wymóg wynikający z Kodeksu:	**Kogo dotyczy (PWDL/ Podmiot przetwarzający/ oba)**	**Wyjaśnienia do wymogu**	**Wskazanie w jaki sposób wymóg został spełniony (wypełnia Podmiot składający oświadczenie lub wniosek)[56]**
Prawidłowe określenie celów i podstaw prawnych przetwarzania.	PWDL	Należy ocenić m.in. treści obowiązków informacyjnych, rejestrów czynności przetwarzania, sprawdzić zasadność pobierania zgody	
Prawidłowy zakres przetwarzania danych, dla którego podstawą nie jest zgoda.	PWDL	Należy w szczególności zweryfikować, czy zakres przetwarzanych danych jest adekwatny, stosowny i ograniczony dla celów przetwarzania	
Prawidłowy zakres przetwarzania danych, dla którego podstawą jest zgoda.	PWDL	Należy w szczególności zwrócić uwagę na zasadność wykorzystania zgody jako podstawy prawnej przetwarzania danych w danym procesie, należy ocenić prawidłowość zbieranych zgód w stosunku do procesu przetwarzania, a także procedurę i okoliczności jej gromadzenia (zapewnienie swobody, niewykorzystywanie stosunku zależności) oraz wycofywania (zwłaszcza łatwość wycofania), sposób realizacji zasady rozliczalności w odniesieniu do zgody	
Prawidłowa identyfikacja podmiotów jako Podmioty przetwarzające/ Administratorzy/ osoby przetwarzające dane z upoważnienia.	Oba*	Należy w szczególności zwrócić uwagę czy podmiot odpowiednio identyfikuje w zawartych przez siebie umowach role i obowiązki związane z przetwarzaniem danych, w tym czy zawiera umowy powierzenia przetwarzania danych z właściwymi podmiotami. Uwaga: możliwe jest uznanie wskazanego wymogu za spełniony przez PWDL, jeżeli występują łącznie następujące okoliczności:	

[56] Należy w sposób syntetyczny wskazać sposób wypełnienia obowiązku, jeśli jest to celowe i zasadne należy również odnieść się do dokumentacji wdrożonej przez podmiot, takiej jak posiadane procedury czy wzory.

		a) ilość zawartych umów, w których zastosowano niewłaściwą klasyfikację jest niewielka (mniejsza niż 20% wszystkich umów związanych z przetwarzaniem danych, których stroną jest podmiot); b) nie jest możliwa zmiana lub rozwiązanie wskazanych umów bez poniesienia istotnego uszczerbku przez PWDL i jednocześnie PWDL oświadcza, że wskazane umowy ulegną rozwiązaniu lub zmianie nie później niż w ciągu roku od dnia złożenia oświadczenia; c) odstępstwo od wskazanego wymogu nie stwarza istotnego ryzyka naruszenia praw i wolności osób w związku z przetwarzaniem ich danych osobowych. *w odniesieniu do Podmiotów przetwarzających należy sprawdzić, czy prawidłowo ustalają swoją rolę w procesie (jako Podmioty przetwarzające), w przypadku nieprawidłowej identyfikacji nie jest możliwe uzyskanie statusu Podmiotu przestrzegającego Kodeksu.	
Prawidłowe zarządzanie zasadami dostępu personelu do danych osobowych Pacjentów.	PWDL	Należy ocenić, w szczególności celowość i niezbędność dostępu danych osobowych Pacjentów ze względu na zadania personelu. Należy zwrócić uwagę, czy te same zadania mogłyby być realizowane bez dostępu do danych, w szczególności do danych sensytywnych. Należy zweryfikować prawidłowość nadawania upoważnień.	
Prawidłowe udostępnianie Dokumentacji medycznej.	Oba*	Należy w szczególności ocenić sposób udostępniania Dokumentacji medycznej, treść upoważnienia do dostępu do Dokumentacji medycznej itp. *wskazany wymóg można analizować w odniesieniu do Podmiotów przetwarzających, które dostarczają rozwiązania techniczne i/lub organizacyjne	

		i uczestniczą w procesie udostępniania Dokumentacji medycznej[57].	
Prawidłowa anonimizacja lub pseudonimizacja danych przed udostępnieniem podmiotom trzecim.	PWDL	Należy w szczególności zweryfikować, czy w przypadku udostępnienia danych podmiotom trzecim, które nie są upoważnione do dostępu do danych osobowych dane zostały poddane skutecznej anonimizacji lub pseudonimizacji, której odwrócenie przez osobę trzecią byłoby niemożliwie bez uzyskania dodatkowych informacji prawnie chronionych w sposób niezgodny z prawem.	
Udostępnianie danych osobowych Pacjentów osobom trzecim w stanie wyższej konieczności, które to osoby nie są upoważnione do dostępu do danych na podstawie przepisów polskiego prawa medycznego (na podstawie art. 9 ust. 2 lit. c) RODO).	PWDL	Należy w szczególności zweryfikować, czy istnieje procedura/ zasady informowania osób trzecich w stanie wyższej konieczności, czy zasady te są zgodne z zapisami Kodeksu.	
Postępowanie w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych.	PWDL	Należy zweryfikować, czy podmiot wdrożył zalecenia wskazane w załączniku nr 3 do Kodeksu.	
Weryfikacja czy podmiot jest zobowiązany do powołania IOD i czy powołał IOD	PWDL	Należy w szczególności zweryfikować, czy PWDL przetwarza dane na dużą skalę zgodnie z Kodeksem	
Weryfikacja czy podmiot zapewnia bezpieczeństwo ochrony danych osobowych	Oba	Należy w szczególności zweryfikować, czy podmiot prawidłowo oszacował poziom ryzyka i czy wdrożył odpowiednie środki zaradcze. Możliwe jest wykorzystanie własnej metodyki analizy ryzyka i własnych zabezpieczeń, przy czym PWDL lub Podmiot przetwarzający muszą wykazać, że przyjęta metodyka zapewnia co najmniej taki sam	

[57] W przypadku Podmiotów przetwarzających, które nie przetwarzają danych w ramach procesu ich udostępniania podmiotom trzecim, w kolumnie obok należy wpisać: „nie dotyczy”.

		poziom bezpieczeństwa jak wskazany w Kodeksie.	
Weryfikacja czy podmiot prowadzi w sposób odpowiedni ocenę skutków dla ochrony danych	Oba*	Należy w szczególności zweryfikować, czy podmiot prawidłowo zweryfikował procesy wymagające przeprowadzenia oceny skutków, a także, czy podmiot prawidłowo oszacował poziom ryzyka i czy wdrożył odpowiednie środki zaradcze. Możliwe jest wykorzystanie własnej metodyki analizy ryzyka i własnych zabezpieczeń, przy czym PWDL lub Podmiot przetwarzający muszą wykazać, że przyjęta metodyka zapewnia co najmniej taki sam poziom bezpieczeństwa jak wskazany w Kodeksie. *w odniesieniu do Podmiotu przetwarzającego weryfikacji podlega spełnienie wymogu wskazanego w pkt. 5.3.6.	
Weryfikacja zasad powierzenia przetwarzania danych	Oba*	W odniesieniu do PWDL należy w szczególności zweryfikować, czy PWDL dokonuje oceny Podmiotów przetwarzających i czy korzysta z usług Podmiotów przetwarzających dających wystarczające gwarancje bezpieczeństwa, należy również zweryfikować czy umowa powierzenia przetwarzania spełnia wymogi określone w RODO, a także czy zapewnia niezakłócone korzystanie z usług oraz możliwość przeprowadzenia audytu zgodnie z Kodeksem. *w odniesieniu do Podmiotu przetwarzającego, należy zweryfikować zawierane przez ten podmiot umowy, ale tylko jeżeli ten podmiot korzysta z przygotowanych przez siebie wystandaryzowanych wzorów umów powierzenia przetwarzania (odniesienie do tych wzorów musi zostać wskazane w ostatniej kolumnie[58]), należy również ocenić relacje tego podmiotu z podprocesorami). Należy w szczególności ocenić spełnienie pkt. 5.4.6. i 5.4.8. Kodeksu. Należy zweryfikować czy Podmiot	

[58] Np. kolumnie obok należy wskazać link, pod którym można pobrać wzór umowy ze wskazaniem jakiej wersji dotyczy oświadczenie.

		przetwarzający zapewnia niezakłócone korzystanie z usług przetwarzania danych. Zmiany we wzorach, które nie są istotne z punktu widzenia ochrony danych osobowych nie wymagają zgłoszenia Komitetowi sterującemu.	
Zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa danych osobowych	Oba	Należy w szczególności zweryfikować poziom wiedzy personelu przetwarzającego dane osobowe, należy również zweryfikować czy PWDL lub Podmiot przetwarzający prowadzą udokumentowane i cykliczne działania w obszarze zwiększenia wiedzy w zakresie bezpieczeństwa danych osobowych.	
Zapewnienie właściwej realizacji praw Pacjentów jako podmiotów danych	PWDL	Należy w szczególności zweryfikować zarówno ogólne kwestie dotyczące realizacji praw, takie jak sposób ustalenia tożsamości Pacjenta, czy forma przekazywania informacji Pacjentowi, jak również należy odnieść się szczegółowo do wszystkich praw i obowiązków wskazanych w Kodeksie (art. 13, 14, 15, 16, 17, 18, 20, 21, 22 RODO)	
Zgodność z prawem procesów wykorzystujących profilowanie lub inne zautomatyzowane przetwarzanie danych	PWDL	Należy w szczególności ocenić, czy PWDL podejmuje decyzje opierające się wyłącznie na zautomatyzowanym przetwarzaniu danych, które to decyzje istotnie wpływają na Pacjentów lub osoby trzecie i zweryfikować zgodność z prawem takiego przetwarzania.	