Załącznik nr 4.

Kwestionariusz oceny podmiotu przetwarzającego dane w imieniu Administratora.

NAZWA ADMINISTRATORA:

SPECJALISTYCZNY SZPITAL im. dra ALFREDA SOKOŁOWSKIEGO w WAŁBRZYCHU

KWESTIONARIUSZ OCENY PODMIOTU PRZETWARZAJĄCEGO DANE W IMIENIU ADMINISTARTORA

(potencjalnego Podmiotu Przetwarzającego na podstawie art. 28 ust. 1 RODO)

A. DANE INFORMACYJNE

NAZWA PODMIOTU	
ADRES/SIEDZIBA	
NIP	
REGON	
KRS	

B. KWESTIONARIUSZ

LP	PYTANIE PODSTAWA PRAWNA RODO	ODPOWIEDŹ			INFORMACJE DODATKOWE, UWAGI PODMIOTU PRZETWARZAJĄCEGO	UWAGI ADO
		TAK	NIE	NIE DOTYCZY		
1.	Czy przepisy prawa wymagają, aby Podmiot przetwarzający wyznaczył inspektora ochrony danych? (art. 37)					
2.	Czy Podmiot przetwarzający wyznaczył inspektora ochrony danych? (art. 37)					
3.	Czy Podmiot przetwarzający wyznaczył inną osobę lub zespół osób odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji? (art. 24)					Proszę wypełnić jeśli odpowiedzi na pytania 1 i 2 są negatywne.
4.	Czy personel Podmiotu przetwarzającego dedykowany do obsługi administratora został przeszkolony z zakresu przepisów o ochronie danych osobowych? (art. 24.)					
5.	Czy fakt przeszkolenia personelu (pkt. 4) jest udokumentowany? (art. 24)					

6.	Czy personel Podmiotu przetwarzającego został przeszkolony w zakresie bezpieczeństwa informatycznego? (art. 24)					
7.	Czy personelowi Podmiotu przetwarzającego wydawane są upoważnienia do przetwarzania danych osobowych? (art. 24,29)					
8.	Czy personel Podmiotu przetwarzającego został zobowiązany do zachowaniu w poufności danych osobowych? (art. 24,28)					
9.	Czy w odniesieniu do Podmiotu przetwarzającego została wydana prawomocna decyzja organu nadzorczego lub wyrok sądu stwierdzający naruszenie zasad ochrony danych osobowych? Czy naruszenie zostało usunięte? (art. 24)					
10.	Czy Podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania? Proszę je wymienić. (art. 40)					
11.	Czy Podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący? (art. 41)					

12.	Czy Podmiot przetwarzający otrzymał certyfikat zgodności z RODO? (art. 42)					
13.	Czy Podmiot przetwarzający posiada inny certyfikat bezpieczeństwa (np. ISO 27001)? Proszę wymienić wraz z nr certyfikacji i terminem ważności. (art. 24)					
14.	Czy Podmiot przetwarzający wdrożył Politykę bezpieczeństwa danych osobowych lub inny dokument opisujący system ochrony danych osobowych oraz procedury postępowania w związku z realizacją wymogów RODO? (art. 24 ust. 2)					
15.	Czy wdrożona instrukcja/procedura postępowania w sytuacji naruszenia ochrony danych osobowych zawiera postanowienia o obowiązku poinformowania Administratora o naruszeniu i o sposobie realizacji tego obowiązku? (art. 24, 33 ust. 2)					
16.	Czy wdrożona instrukcja/procedura postępowania w sytuacji naruszenia ochrony danych osobowych zawiera zapisy dotyczące obowiązku podjęcia środków w celu zaradzenia naruszeniu (w tym					

	minimalizowania skutków)? (art. 24, 33 ust. 3 lit. d)					
17.	Czy Podmiot przetwarzający prowadzi ewidencję naruszeń ochrony danych osobowych? (art. 24, 33 ust. 5)					
18.	Czy Podmiot przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych (jako ADO) oraz rejestr kategorii czynności przetwarzania danych jako podmiot przetwarzający? (art. 30)					
19.	Czy Podmiot przetwarzający wdrożył odpowiednie środki organizacyjne i techniczne (np. instrukcja, procedura, zakres odpowiedzialności pracowników, funkcjonalność systemu IT) przeznaczone do pomocy Administratorowi w realizacji praw osób, których dane dotyczą? (art. 15-22, 28 ust.3 lit. e)					
20.	Czy Podmiot przetwarzający realizuje proces analizy ryzyka oraz analizy naruszenia praw lub wolności osób fizycznych (DPiA)? (art. 24, 32, 35)					
21.	Czy Podmiot przetwarzający wdrożył zabezpieczenia we własnym systemie					

	informatycznym adekwatne do wyników szacowania ryzyka oraz DPiA? (art. 24, 32)					
22.	Czy system informatyczny Podmiotu przetwarzającego zapewnia pełną rozliczalność działań jego użytkowników? (art. 24, 32)					
23.	Czy Podmiot przetwarzający przekazuje dane osobowe do państwa trzeciego, na zasadach określonych w rozdziale V RODO? Proszę wskazać na jakich zasadach (art. 44 – 49, Decyzja Wykonawcza Komisji (UE) 2021/914 z dnia 04.062021r.)					
24.	Czy Podmiot przetwarzający wdrożył „Plan Ciągłości Działania” ? (art. 24, 32)					
25.	Czy Podmiot przetwarzający stosuje regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych ? W jakiej formie są dokumentowane? (art. 32)					
26.	Czy Podmiot przetwarzający korzysta w ramach powierzenia lub ma zamiar korzystać z usług innych podmiotów (tzw. „pod-powierzających” lub dalszych podmiotów przetwarzających)? (art. 24, 28)					

27.	Czy Podmiot przetwarzający przed nawiązaniem współpracy z tzw. „pod-powierzającymi” dokonuje jego weryfikacji pod kątem zdolności do zapewnienia ochrony danych osobowych ? (art. 28)					
28.	Czy Podmiot przetwarzający z pod-powierzającymi ma zawarte stosowne umowy lub inne formy udokumentowanego przetwarzania w jego imieniu ? (art. 28)					Proszę wypełnić w przypadku odpowiedzi twierdzącej w pkt. 26

C. INFORMACJE KOŃCOWE

DATA WYPEŁNIENIA	
IMIĘ I NAZWISKO OSOBY AUTORYZUJĄCEJ DOKUMENT W IMIENIU PODMIOTU PRZETWARZAJĄCEGO PEŁNIONA FUNKCJA/STANOWISKO	

LICZBA STRON KWESTIONARIUSZA	

D. OCENA ADMINISTRATORA

IMIĘ I NAZWISKO OSOBY WERYFIKUJĄCEJ DOKUMENT W IMIENIU ADMINISTARTORA DANYCH OSOBOWYCH	
DATA ANALIZY/OCENY	
REKOMENDOWANA DECYZJA	