

**Karta oceny podmiotu przetwarzającego**

<b>Dane administratora:</b> <b>Narodowy Instytut Onkologii im. M. Skłodowskiej-Curie, Państwowy Instytut Badawczy Oddział w Krakowie ul. Garncarska 11 31-115 Kraków</b>	<b>Dane przetwarzającego:</b> ..... ..... ..... .....
<b>Okres umowy:</b> ..... .....	<b>Rodzaj usługi/czynności:</b> ..... .....

LP	PYTANIE	ODPOWIEDŹ
1	W jakiej formie będziesz przetwarzał powierzone dane osobowe (papierowej, elektronicznej, w obu formach) ?	
2	Czy dane będą poddane archiwizacji po okresie realizacji umowy, a jeśli tak to na jakiej podstawie?	
3	W jaki sposób planowane jest zwrócenie danych po okresie realizacji umowy?	
4	Czy przy realizacji umowy, zamierzasz korzystać z innych podmiotów (swoich podwykonawców)?	
5	Czy zamierzasz przekazywać powierzone dane osobowe do państwa trzeciego poza EOG?	
6	Czy wyznaczyłeś Inspektora Ochrony Danych a jeśli nie to czy dokonałeś oceny pod kątem obowiązku wyznaczenia IOD na podstawie art. 37 ust 1 RODO?	
7	Jeśli nie wyznaczyłeś Inspektora Ochrony Danych to czy samodzielnie jako podmiot przetwarzający wykonujesz zadania IOD określone w art. 39 RODO?	
8	Czy prowadzisz i dokumentujesz szkolenia z zakresu ochrony danych osobowych dla personelu dopuszczonego do przetwarzania danych osobowych?	
9	Czy opracowałeś i wdrożyłeś politykę ochrony danych osobowych lub inne instrukcje i procedury dotyczące sposobu przetwarzania i zabezpieczenia danych osobowych?	

10	Czy wdrożyłeś system zarządzania bezpieczeństwem informacji w oparciu o uznane międzynarodowe normy (np. ISO 27001)?	
11	Czy zastosowałeś adekwatne zabezpieczenia w postaci środków technicznych i organizacyjnych dla ochrony danych osobowych z uwzględnieniem ryzyka i zagrożeń dla bezpieczeństwa danych?	
12	Czy do przetwarzania danych osobowych dopuszczasz wyłącznie osoby upoważnione, zobowiązane do zachowania danych w tajemnicy i jesteś w stanie to wykazać?	
13	Czy jesteś w stanie zapewnić administratorowi pomoc w wywiązaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą w zakresie wykonywania jej praw określonych w Rozdziale III RODO?	
14	Czy wdrożyłeś i zakomunikowałeś procedurę dotyczącą reagowania na naruszenia ochrony danych osobowych i jesteś w stanie dokonać powiadomienia administratora o naruszeniu w ciągu 24 godzin od stwierdzenia naruszenia?	
15	Czy prowadzisz rejestr naruszeń ochrony danych osobowych i udzielić administratorowi informacji o zidentyfikowanych dotychczas naruszeniach?	
16	Czy jesteś gotowy udzielać administratorowi wszelkich informacji w przypadku naruszenia ochrony danych osobowych w szczególności informacji, o których mowa w art. 33 ust. 2 RODO?	
17	Czy prowadzisz rejestr kategorii czynności przetwarzania w imieniu administratora, o którym mowa w art. 30 ust. 2 RODO?	
18	Czy w przeciągu ostatnich 12 miesięcy poddałeś się ocenie podmiotu zewnętrznego w zakresie uwzględniającym bezpieczeństwo danych osobowych (np. audyt zewnętrzny ISO 27001, inne audyty technologiczne) i czy jesteś gotowy udzielić informacji dotyczących spostrzeżeń i niezgodności, które zostały ujawnione w wyniku audytu?	
19	Czy zapewniasz środki fizycznej ochrony dostępu do obszarów, w których przetwarzasz dane osobowe a jeśli tak jakie to środki (np. dostęp na kod, zamykanie pomieszczeń na klucz, system przeciwwłamaniowy, itp.)?	
20	Czy stosujesz środki ochrony teleinformatycznej przy przetwarzaniu danych osobowych w systemach informatycznych i jakie to środki (firewall, złożone hasła, uwierzytelnianie wieloetapowe, itp.)?	

.....  
Data i podpis wypełniającego