

## Formularz audytowy podmiotu przetwarzającego

Podmiot Przetwarzający: \_\_\_\_\_

Administrator danych: Wojewódzki Szpital Specjalistyczny im. Bł. Ks. Jerzego Popiełuszki we Włocławku  
ul. Wieniecka 49, 87-800 Włocławek

W związku z koniecznością potwierdzenia czy Podmiot Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, uprzejmie proszę o udzielenie odpowiedzi na poniższe pytania:

Powołanie Inspektora Ochrony Danych lub osoby o podobnych kompetencjach i zadaniach					
L.p.	TREŚĆ PYTANIA	TAK/NIE	ODPOWIEDŹ	STOPIEŃ ZGODNOŚCI (wypełnia ADO)	REKOMENDACJE (wypełnia ADO)
1	Czy Podmiot Przetwarzający dokonał prawidłowej analizy istnienia obowiązku wyznaczenia Inspektora Ochrony Danych (IOD)?				
2	Czy na Podmiocie Przetwarzającym spoczywa obowiązek wyznaczenia IDO?				
3	Czy Podmiot Przetwarzający wyznaczył IOD?				
4	Jeżeli IOD nie został wyznaczony, to czy zadania dotyczące zapewnienia zgodności z przepisami o ochronie danych osobowych w ramach organizacji wykonuje inna wyznaczona osoba?				
Bezpieczeństwo zasobów ludzkich					
L.p.	TREŚĆ PYTANIA	TAK/NIE	ODPOWIEDŹ	STOPIEŃ ZGODNOŚCI (wypełnia ADO)	REKOMENDACJE (wypełnia ADO)

## Formularz audytowy podmiotu przetwarzającego

1	Czy osoby dopuszczone przez Podmiot Przetwarzający do przetwarzania danych osobowych zostały przeszkolone w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego?				
2	Czy Podmiot Przetwarzający dokumentuje przeprowadzenie szkoleń w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego?				
3	Czy osoby dopuszczone przez Podmiot Przetwarzający do przetwarzania danych osobowych są upoważnione do ich przetwarzania? Czy działają na polecenie Administratora?		Proszę opisać sposób dokumentowania upoważnień:		
4	Czy Podmiot przetwarzający dokumentuje nadawanie upoważnień do przetwarzania danych osobowych?				
5	Czy osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?				
6	Czy Podmiot Przetwarzający dokumentuje fakt zobowiązania się do zachowania tajemnicy przez osoby przetwarzające dane?		Proszę opisać sposób dokumentowania faktu zobowiązania do zachowania tajemnicy osób przetwarzających dane osobowe:		
7	Czy Podmiot przetwarzający prowadzi ewidencję nadanych upoważnień?				

## Formularz audytowy podmiotu przetwarzającego

Naruszenie ochrony danych osobowych oraz realizacja praw osób, których dane dotyczą					
L.p.	TREŚĆ PYTANIA	TAK/NIE	UWAGI	STOPIEŃ ZGODNOŚCI (wypełnia ADO)	REKOMENDACJE (wypełnia ADO)
1	Czy Podmiot Przetwarzający jest w stanie zapewnić Administratorowi pomoc w wywiązaniu się z obowiązku zgłaszania naruszeń ochrony danych osobowych organowi nadzorcemu oraz zawiadamiania osób fizycznych o naruszeniach, w odniesieniu do powierzonych danych osobowych?				
2	Czy Podmiot Przetwarzający wdrożył procedurę lub inną dokumentację dotyczącą postępowania w przypadku naruszenia ochrony danych?		Proszę opisać rodzaj wdrożonej dokumentacji:		
3	Czy Podmiot Przetwarzający jest w stanie zapewnić Administratorowi pomoc w wywiązaniu się z obowiązku odpowiadania na żądania osoby fizycznej w zakresie wykonywania jej praw przyznanych na mocy RODO - w odniesieniu do powierzonych danych osobowych?				
Dalsze powierzenie przetwarzania powierzonych danych osobowych					
L.p.	TREŚĆ PYTANIA	TAK/NIE	UWAGI	STOPIEŃ ZGODNOŚCI (wypełnia ADO)	REKOMENDACJE (wypełnia ADO)
1	Czy w ramach realizacji usług zleconych przez Administratora Podmiot Przetwarzający korzysta lub zamierza korzystać z usług podwykonawców, którym zostały lub zostaną dalej powierzone dane osobowe przekazane przez Administratora (tzw. Podpowierzenie)?		Proszę podać nazwę podmiotów, którym dane są lub będą przekazywane oraz zakres podpowierzanych danych, informacje o rodzaju usług jakie są lub będą świadczone przez wykonawców:		

## Formularz audytowy podmiotu przetwarzającego

2	Czy Podmiot Przetwarzający zamierza lub podpowierzył dane osobowe podwykonawcom zgodnie z wymogami RODO?				
3	Czy Podmiot Przetwarzający zobowiązał podwykonawców do zapewnienia takich samych środków bezpieczeństwa, co Podmiot Przetwarzający?				
4	Czy Podmiot Przetwarzający zamierza przekazywać powierzone mu dane osobowe dalszym podmiotom przetwarzającym poza Europejski Obszar Gospodarczy?		Do jakich krajów spoza EOG podmiot zamierza przekazywać dane osobowe i na jakiej podstawie prawnej, ewentualnie z zastosowaniem jakich zabezpieczeń?		
5	Czy podmiot przetwarzający posiada procedurę/instrukcję/mechanizm zwrotu powierzonych danych Administratorowi zgodnie z art. 28 RODO?				

### Bezpieczeństwo przetwarzania danych

L.p.	TREŚĆ PYTANIA	TAK/NIE	UWAGI	STOPIEŃ ZGODNOŚCI (wypełnia ADO)	REKOMENDACJE (wypełnia ADO)
1	Czy Podmiot Przetwarzający posiada wdrożony proces szacowania ryzyka naruszenia praw i wolności osób fizycznych (identyfikacja, analiza i ocena ryzyka)?		Proszę wskazać według jakiej metodologii przeprowadza się analizę ryzyka?		
2	Czy Podmiot Przetwarzający przeprowadził analizę ryzyka naruszenia praw i wolności osób fizycznych dla czynności, w ramach których doszło do przetwarzania danych				

## Formularz audytowy podmiotu przetwarzającego

	osobowych powierzonych mu przez Administratora?				
3	Czy w oparciu o przeprowadzoną analizę ryzyka naruszenia praw i wolności osób fizycznych dla czynności, w ramach których doszło do przetwarzania danych osobowych powierzonych mu przez Administratora, Podmiot Przetwarzający oświadcza, że ryzyko jest niskie tzn. akceptowalne?				
4	Czy Podmiot Przetwarzający zobowiązuje się poinformować Administratora w przypadku zmiany poziomu stwierdzonego ryzyka naruszenia praw i wolności osób fizycznych?				
5	Czy Podmiot Przetwarzający zapewnia adekwatny do ryzyka naruszenia praw i wolności osób fizycznych poziom bezpieczeństwa powierzonych danych w szczególności zabezpieczył je przed przypadkowym zniszczeniem, utratą, modyfikacją czy nieuprawnionym ujawnieniem, zgodnie z art. 25 RODO?		Proszę opisać:		
6	Czy Podmiot Przetwarzający wdrożył adekwatne do ryzyka naruszenia praw i wolności osób fizycznych środki ochrony na wypadek awarii, takie jak kopie zapasowe?		Proszę opisać:		
7	Czy Podmiot Przetwarzający przechodzi regularne audyty z zakresu bezpieczeństwa danych mające na celu ocenę skuteczności zastosowanych środków technicznych i organizacyjnych?		Proszę opisać:		
8	Czy podmiot przetwarzający realizuje prawa osób, których dane dotyczą zgodnie z przepisami od art. 15 do art. 22 RODO?				
9	Czy oprogramowania stosowane przez podmiot przetwarzający są na bieżąco aktualizowane a także czy według najlepszej				

## Formularz audytowy podmiotu przetwarzającego

	wiedzy podmiotu przetwarzającego są pozyskane i używane zgodnie z prawem (w przypadku przetwarzania danych w systemach informatycznych)?				
10	Czy podmiot przetwarzający realizuje obowiązek prowadzenia rejestru kategorii czynności przetwarzania zgodnie z art. 30 RODO? W przypadku odpowiedzi przeczącej proszę o podanie przyczyny i jej uzasadnienie.				
11	<p>Czy podmiot przetwarzający stosuje środki bezpieczeństwa przewidziane w art. 32 RODO dotyczące:</p> <p>a) pseudonimizacji i szyfrowania powierzonych danych,</p> <p>b) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania powierzonych danych,</p> <p>c) zdolności do szybkiego przywrócenia dostępności danych,</p> <p>d) prowadzenia regularnego testowania, mieszania i oceniania skuteczności zastosowanych zabezpieczeń?</p>				
<p><b>Poniższą część Ankiety należy wypełnić, jeżeli dojdzie do powierzenia przetwarzania danych osobowych stanowiących Dokumentację medyczną</b></p>					
L.P.	TREŚĆ PYTANIA	TAK/NIE	ODPOWIEDŹ	STOPIEŃ ZGODNOŚCI (wypełnia ADO)	REKOMENDACJE (wypełnia ADO)
1	Czy podmiot przetwarzający systematycznie szacuje ryzyko zagrożeń oraz zarządza tym ryzykiem?				
2	Czy dokumentacja medyczna jest zabezpieczona poprzez zapewnienie jej dostępności wyłącznie osobom uprawnionym oraz czy zastosowano metody i środki ochrony dokumentacji, których				

## Formularz audytowy podmiotu przetwarzającego

	skuteczność w czasie ich zastosowania jest powszechnie uznana (w przypadku gdy ma to zastosowanie)?				
<b>3</b>	Czy podmiot przetwarzający zapewnia bezpieczeństwo dokumentacji medycznej zarówno w formie papierowej jak i w postaci elektronicznej zgodnie z §1 ust. 5 Rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (w przypadku gdy ma to zastosowanie)?				
<b>4</b>	Czy system informatyczny, w którym będzie przetwarzana dokumentacja medyczna zapewnia spełnienie wymogów określonych w §1 ust. 6 Rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (w przypadku gdy ma to zastosowanie)?				

*Data wypełnienia formularza:*

*Imię, Nazwisko osoby wypełniającej formularz:*

.....

.....