

Wzór ankiety dla Przetwarzającego

WERYFIKACJA PODMIOTU, KTÓREMU MA ZOSTAĆ POWIERZONE PRZETWARZANIE DANYCH OSOBOWYCH (dalej jako „Przetwarzający”)

Dane podmiotu, któremu Administrator zamierza powierzyć Dane osobowe do przetwarzania w związku z wykonaniem Umowy głównej*.

Firma (nazwa):

Adres (siedziba):

Osoba wypełniająca ankietę: []; stanowisko: []

Numer KRS: [];

NIP: [], Regon: []

*uzupełnić/skreślić właściwe pola

Pytania ogólne z zakresu ochrony Danych osobowych

LP.	TREŚĆ PYTANIA	TAK/NIE/ NIE DOTYCZY	UWAGI/KOMENTARZE/ UZASADNIENIE
1.	Czy firma posiada i stosuje procedury ochrony Danych osobowych (np. politykę bezpieczeństwa Danych osobowych)?		
2.	Czy prowadzony jest Rejestr Kategorii Czynności Przetwarzania?		
3.	Czy osoby wykonujące operacje na powierzonych przez Administratora Danych osobowych zostały upoważnione do ich przetwarzania?		
4.	Czy osoby wykonujące powyższe operacje zostały odpowiednio przeszkolone w zakresie ochrony Danych oraz zapoznane z właściwymi zasadami ich przetwarzania (szczególnie w zakresie zachowania poufności, integralności i bezpieczeństwa)?		
5.	Czy szkolenia, o których mowa w powyższym punkcie są cykliczne?		
6.	Czy osoby upoważnione do przetwarzania powierzonych Danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?		
7.	Czy Przetwarzający korzysta z usług podwykonawców w zakresie przetwarzania Danych osobowych (w tym ich zabezpieczania)?		

8.	Czy Przetwarzający zawarł z podwykonawcami wykonującymi operacje na powierzonych Danych osobowych pisemne (w tym elektroniczne) Umowa powierzenia Danych osobowych, nakładające na nich te same obowiązki ochrony Danych, jak określone w Umowach powierzenia zawartych z odpowiednimi administratorami Danych?		
9.	Czy wyznaczony został Inspektor Ochrony Danych lub inna osoba do wykonywania zadań związanych z zapewnieniem ochrony Danych osobowych?		
10.	Czy prowadzone są okresowe wewnętrzne audyty bezpieczeństwa dla czynności przetwarzania Danych osobowych?		
Pytania szczegółowe z zakresu ochrony Danych osobowych			
LP.	TREŚĆ PYTANIA	TAK/NIE/NIE DOTYCZY	UWAGI/KOMENTARZE/UZASADNIENIE
11.	Czy Przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO?		
12.	Czy Przetwarzający posiada zatwierdzony mechanizm certyfikacji lub znak jakości w zakresie ochrony Danych osobowych, o których mowa w art. 42 RODO?		
13.	Czy Dane powierzone będą przetwarzane poza EOG?		
14.	Czy zapewniono mechanizm legalizujący transfer Danych poza EOG?		
15.	Czy realizacja usług dla Administratora będzie wymagała profilowania podmiotów Danych?		
16.	Czy w ramach realizacji usług dla Administratora zakładają Państwo zautomatyzowane podejmowanie decyzji wobec podmiotów Danych?		
17.	Czy w celu zaplanowania środków bezpieczeństwa przeprowadzili Państwo analizę ryzyka dla operacji przetwarzania wykonywanych dla Administratora?		
18.	Czy zostały wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony Danych osobowych?		

20.	Czy prowadzony jest Rejestr naruszeń ochrony Danych osobowych?		
21.	Czy wdrożono instrukcję postępowania w przypadku sytuacji naruszenia ochrony Danych osobowych?		
22.	Czy zgodnie z tą Instrukcją, zagwarantowano przekazanie Administratorowi informacji o incydencie w ciągu 24 godzin od stwierdzenia naruszenia?		
23.	Czy przeprowadzana jest ocena skutków planowanych operacji przetwarzania dla Danych osobowych (DPIA)?		
24.	Czy procesy przetwarzania Danych były już przedmiotem zewnętrznych audytów lub kontroli, np. PUODO?		
25.	Czy zewnętrzna kontrola lub audyt, o których mowa w powyższym punkcie miała miejsce w ciągu ostatnich dwóch lat?		
26.	Czy w ciągu ostatniego roku zaistniało zdarzenie związane z naruszeniem Danych osobowych?		
27.	Czy wdrożono normy zarządzania w zakresie ochrony informacji (np. ISO)? Czy Przetwarzający posiada stosowny certyfikat?		
28.	Czy wprowadzone zostały środki kontroli dostępu fizycznego do pomieszczeń, w których znajdują się Dane osobowe?		
29.	Czy wprowadzone zostały techniczne środki ochrony Danych osobowych?		
30.	Czy wprowadzone zostały prawne środki ochrony Danych osobowych?		
29.	Czy dostęp do pomieszczeń lub systemów informatycznych, w których znajdują się Dane osobowe ograniczony jest wyłącznie do osób upoważnionych?		
30.	Czy Dane osobowe znajdujące się na nośnikach fizycznych (np. na wydrukach) przechowywane są po godzinach pracy przedsiębiorstwa w zamkniętych pojemnikach (np. szafkach, szufladach) bez możliwości dostępu do nich osób nieupoważnionych?		

31.	Czy w organizacji Przetwarzającego stosowana jest zasada tzw. "czystego biurka" i „czystego ekranu”?		
32.	Czy Przetwarzający wdraża nowe rozwiązania zgodnie z zasadą "privacy by design", zgodnie z art. 25 ust. 1 RODO?		
33.	Czy Przetwarzający wdraża nowe rozwiązania zgodnie z zasadą "privacy by default", zgodnie z art. 25 ust. 2 RODO?		
34.	Czy Przetwarzający posiada wdrożone rozwiązania umożliwiające realizację praw i żądań osób, których Dane przetwarza w imieniu i na zlecenie Administratora?		
Pytania z zakresu bezpieczeństwa infrastruktury i systemów IT			
LP.	TREŚĆ PYTANIA	TAK/NIE/ NIE DOTYCZY	UWAGI/KOMENTARZE/ UZASADNIENIE
35.	Czy organizacja wdrożyła instrukcję zarządzania systemami IT służącymi do przetwarzania Danych osobowych lub inne regulacje wewnętrzne dot. zasad zarządzania infrastrukturą IT?		
36.	Czy systemy IT Przetwarzający, w których dokonywane jest przetwarzanie Danych na zlecenie Administratora, zapewniają rozliczalność operacji wykonywanych na Danych osobowych, tzn. czy odnotowują nazwę użytkownika, datę oraz charakter operacji wykonanej na konkretnym rekordzie w bazie?		
37.	Czy dostęp do systemów IT wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		
38.	Czy wykorzystywane przez Przetwarzającego systemy IT automatycznie wymagają okresowej zmiany hasła?		
39.	Czy komputery i systemy IT w organizacji Przetwarzającego działają z aktywnym i zaktualizowanym programem antywirusowym?		
40.	Czy komputery i systemy IT w organizacji Przetwarzającego są chronione przed nieautoryzowanym dostępem do sieci za pomocą firewalla (sieci lub hosta)?		
41.	Czy komputery i systemy IT w organizacji Przetwarzającego są regularnie aktualizowane?		
42.	Czy sieci bezprzewodowe w organizacji Przetwarzającego są szyfrowane i wymagające kodu dostępu lub podobnego zabezpieczenia, aby zapobiec nieautoryzowanemu dostępowi do sieci i podsłuchom?		

.....

Data i Podpis osoby uprawnionej do reprezentacji Przetwarzającego