

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI PRZEZ WYKONAWCĘ

Ankieta

Nazwa wykonawcy:

Dane kontaktowe: tel., e-mail:

Sporządzający ankietę:

Data opracowania:

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
1.	Czy w bieżącym roku lub w poprzednich 3 latach świadczono na rzecz innych podmiotów usługi związane z przetwarzaniem lub z ochroną informacji, w tym danych osobowych?	TAK NIE	Jeśli TAK, to proszę podać liczbę obsługiwanych podmiotów w roku bieżącym i ich liczbę w każdym z 3 lat poprzedzających rok bieżący.
2.	Czy planowane przetwarzanie informacji, realizowane będzie, choćby w ograniczonym zakresie, poza Europejskim Obszarem Gospodarczym (EOG)?	TAK NIE	Jeśli TAK, to proszę podać kraje i powody transferu danych. Jeśli NIE, Opis nie jest wymagany.
3.	Czy świadczone usługi związane z przetwarzaniem informacji, w tym danych osobowych, realizowane będą, choćby częściowo, w ramach pracy zdalnej lub hybrydowej?	TAK NIE	Jeśli TAK, to w jaki zakresie (wyłącznie / częściowo zdalnie / sporadycznie)? Jeśli NIE, Opis nie jest wymagany.
4.	Czy wdrożono i czy są stosowane wewnętrzne wymagania dotyczące pracy zdalnej i hybrydowej?	TAK NIE	Jeśli TAK, Opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?
5.	Czy wdrożono i czy są stosowane wewnętrzne wymagania dotyczące użytkowania urządzeń mobilnych?	TAK NIE	Jeśli TAK, Opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?
6.	Czy do planowanego przetwarzania informacji będą wykorzystywane urządzenia i oprogramowanie komputerowe pozostające w wyłącznej dyspozycji organizacji (TAK), czy dopuszczane będą też inne, w tym prywatne pracowników (NIE)?	TAK NIE	Jeśli TAK, Opis nie jest wymagany. Jeśli NIE, to na jakich zasadach?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
7.	Czy obowiązek prawny wyznaczenia osoby do kontaktów z właściwym CSIRT (Computer Security Incident Response Team) (NASK / GOV / MON / KNF) ma zastosowanie?	TAK NIE	Opis nie jest wymagany.
8.	Czy wyznaczono osobę do kontaktów z właściwym CSIRT (Computer Security Incident Response Team) (NASK / GOV / MON / KNF)?	TAK NIE NIE DOTYCZY	Jeśli TAK, to kiedy? Proszę podać datę. Jeśli TAK i wewnętrznie, to proszę podać nazwę stanowiska pracy lub funkcji zgłoszonej osoby. Jeśli TAK i zewnętrznie, to proszę podać nazwę podmiotu zewnętrznego oraz nazwę stanowiska pracy lub funkcji zgłoszonej osoby, jeśli zostało to określone przez podmiot zewnętrzny. Jeśli NIE lub NIE DOTYCZY, Opis nie jest wymagany.
9.	Czy w bieżącym roku lub w poprzednich 3 latach wystąpiły incydenty cyberbezpieczeństwa?	TAK NIE NIE DOTYCZY	Jeśli TAK, to do ilu w roku bieżącym i do ilu w każdym z 3 lat poprzedzających rok bieżący i czy incydenty te zostały zarejestrowane wewnętrznie. Jeśli NIE, Opis nie jest wymagany.
10.	Czy w bieżącym roku lub w poprzednich 3 latach dokonywano zgłoszeń incydentów cyberbezpieczeństwa do właściwego CSIRT (NASK / GOV / MON / KNF)?	TAK NIE NIE DOTYCZY	Jeśli TAK, to ilu w roku bieżącym i ilu w każdym z 3 lat poprzedzających rok bieżący i czy incydenty te zostały zarejestrowane wewnętrznie. Jeśli NIE lub NIE DOTYCZY, Opis nie jest wymagany.
11.	Czy wdrożono wewnętrzne wymagania dotyczące zgłoszeń i obsługi incydentów cyberbezpieczeństwa?	TAK NIE NIE DOTYCZY	Jeśli TAK lub NIE DOTYCZY, to opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?
12.	Czy obowiązek prawny wyznaczenia inspektora ochrony danych (IOD) ma zastosowanie?	TAK NIE	Opis nie jest wymagany.

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
13.	Czy wyznaczono inspektora ochrony danych (IOD)?	TAK NIE	Jeśli TAK, to kiedy? Proszę podać datę. Jeśli TAK i wewnętrznie, to proszę podać nazwę stanowiska pracy lub funkcji wyznaczonej osoby, jeśli osoba ta realizuje również obowiązki inne niż wynikające z pełnienia funkcji IOD. Jeśli TAK i zewnętrznie, to proszę podać nazwę podmiotu zewnętrznego. Jeśli NIE, to z jakiego powodu?
14.	Jeśli nie wyznaczono inspektora ochrony danych (IOD), to czy obowiązki prawne w zakresie ochrony danych osobowych realizowane są przy wsparciu innego personelu?	TAK NIE	Jeśli TAK, to proszę podać nazwę lub nazwy stanowisk pracy albo funkcji odpowiedzialnych za realizację obowiązków w zakresie ochrony danych osobowych. Jeśli NIE, Opis nie jest wymagany.
15.	Czy w bieżącym roku lub w poprzednich 3 latach dochodziło do naruszeń ochrony danych osobowych?	TAK NIE	Jeśli TAK, to do ilu w roku bieżącym i do ilu w każdym z 3 lat poprzedzających rok bieżący, i czy incydenty te zostały zarejestrowane wewnętrznie. Jeśli NIE, Opis nie jest wymagany.
16.	Czy w bieżącym roku lub w poprzednich 3 latach dokonywano zgłoszeń incydentów naruszenia danych osobowych do PUODO?	TAK NIE NIE DOTYCZY	Jeśli TAK, to do ilu w roku bieżącym i do ilu w każdym z 3 lat poprzedzających rok bieżący i czy incydenty te zostały zarejestrowane wewnętrznie. Jeśli NIE DOTYCZY, Opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?
17.	Czy wdrożono wewnętrzne wymagania dotyczące zgłoszeń i obsługi naruszeń ochrony danych osobowych?	TAK NIE	Jeśli TAK, to jakie? Jeśli NIE, to z jakiego powodu?
18.	Czy wdrożono politykę ochrony danych osobowych lub inne wewnętrzne wymagania regulacyjne w tym zakresie?	TAK NIE	Jeśli TAK i nie politykę ochrony danych osobowych, to proszę podać nazwy i zakresy regulacyjne wdrożonych wymagań. Jeśli NIE, to z jakiego powodu?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
19.	Czy obowiązek prawny wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI) ma zastosowanie?	TAK NIE	Opis nie jest wymagany.
20.	Czy wdrożono system zarządzania bezpieczeństwem informacji (SZBI)?	TAK NIE	Jeśli TAK, to od kiedy? Proszę podać datę. Jeśli TAK, to czy SZBI jest zgodny z KRI / ISO/IEC 27001 / NSC?
21.	Czy powołano osobę odpowiedzialną za nadzór nad systemem zarządzania bezpieczeństwem informacji (SZBI)?	TAK NIE NIE DOTYCZY	Jeśli TAK, to kiedy? Proszę podać datę. Jeśli TAK i wewnętrznie, to proszę podać nazwę stanowiska pracy lub funkcji wyznaczonej osoby, jeśli osoba ta realizuje również obowiązki inne, niż wynikające z nadzoru nad systemem zarządzania bezpieczeństwem informacji (SZBI). Jeśli TAK i zewnętrznie, to proszę podać nazwę podmiotu zewnętrznego. Jeśli NIE, to z jakiego powodu? Jeśli NIE DOTYCZY, Opis nie jest wymagany.
22.	Czy w bieżącym roku lub w poprzednich 3 latach dochodziło do incydentów lub zdarzeń związanych z bezpieczeństwem informacji?	TAK NIE	Jeśli TAK, to do ilu w roku bieżącym i do ilu w każdym z 3 lat poprzedzających rok bieżący, i czy incydenty te zostały zarejestrowane wewnętrznie. Jeśli NIE, Opis nie jest wymagany.
23.	Czy wdrożono wewnętrzne wymagania dotyczące zgłoszeń i obsługi incydentów, zdarzeń, niezgodności i słabości systemu zarządzania bezpieczeństwem informacji (SZBI)?	TAK NIE NIE DOTYCZY	Jeśli TAK lub NIE DOTYCZY, Opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
24.	Czy powołano administratora systemów informatycznych (ASI)?	TAK NIE	Jeśli TAK, to kiedy? Proszę podać datę. Jeśli TAK i wewnętrznie, to proszę podać nazwę stanowiska pracy lub funkcji wyznaczonej osoby, jeśli osoba ta realizuje również obowiązki inne, niż wynikające z pełnienia funkcji ASI. Analogicznie proszę podać informacje o zastępcy lub zastępcach ASI, jeśli zostali wyznaczeni. Jeśli TAK i zewnętrznie, to proszę podać nazwę podmiotu zewnętrznego. Jeśli NIE, to z jakiego powodu?
25.	Czy stosowane są zatwierdzone mechanizmy certyfikacji związane z przetwarzaniem informacji, w tym danych osobowych?	TAK NIE	Jeśli TAK, to proszę podać jakiego rodzaju (27001 / 27701 / 22301 / inne) oraz ich zakresy stosowania. Jeśli NIE, Opis nie jest wymagany.
26.	Czy stosowany jest zatwierdzony kodeks postępowania dla ochrony danych osobowych?	TAK NIE	Jeśli TAK, to należy podać jego nazwę oraz zakres stosowania. Jeśli NIE, Opis nie jest wymagany.
27.	Czy upoważniane są osoby, które przetwarzają informacje, w tym dane osobowe?	TAK NIE	Jeśli TAK, to w jaki sposób? Proszę podać, czy poprzez określanie zakresów czynności (obowiązków), imienne upoważnienia, czy w inny sposób? Jeśli NIE, to z jakiego powodu?
28.	Czy osoby, które przetwarzają informacje, w tym dane osobowe, zobowiązane są do zachowania ich w poufności / tajemnicy?	TAK NIE	Jeśli TAK, to w jaki sposób? Czy złożyły pisemne oświadczenia woli w tym zakresie? Jeśli NIE, to z jakiego powodu?
29.	Czy prowadzone są działania uświadamiające w zakresie bezpieczeństwa i ochrony informacji, w tym danych osobowych, w stosunku do osób, które je przetwarzają?	TAK NIE	Jeśli TAK, to w jaki sposób? Jeśli TAK, to kiedy ostatnio i czy okresowo? Proszę podać daty z roku bieżącego i z 3 lat poprzedzających rok bieżący. Jeśli NIE, to z jakiego powodu?
30.	Czy zawierane są umowy o zachowaniu poufności (NDA), gdy ma to zastosowanie?	TAK NIE	Jeśli TAK lub NIE DOTYCZY, to opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
31.	Czy zawierane są umowy przetwarzania danych osobowych w imieniu administratora (umowy powierzenia przetwarzania), gdy ma to zastosowanie, albo wymagania w tym zakresie określone są w innych instrumentach prawnych?	TAK NIE	Jeśli TAK lub NIE DOTYCZY, to opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?
32.	Czy wdrożono środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji, w tym danych osobowych, przetwarzanych w systemach informacyjnych?	TAK NIE	Jeśli TAK, to jakiego rodzaju (oprogramowanie antywirusowe, firewall, AD, ERP, SOC, IDS/IPS (UTM), DPL, UDR, EDR/XDR, SIEM, DMZ itp., itd.)? Jeśli NIE, to z jakiego powodu?
33.	Czy wdrożono i stosowane są wewnętrzne wymagania dotyczące zabezpieczania informacji chronionych przesyłanych drogą elektroniczną i czy oraz w jaki sposób informacje te są zabezpieczane?	TAK NIE	Jeśli TAK, to w jaki sposób? Proszę określić rodzaj wdrożonych środków technicznych i organizacyjnych oraz wskazać dokumenty wewnętrzne, które regulują wymagania w tym zakresie. Jeśli NIE, to z jakiego powodu?
34.	Czy wdrożono i czy są stosowane wewnętrzne wymagania dotyczące wykonywania, testowania, przechowywania i zabezpieczania kopii informacji i systemów?	TAK NIE	Jeśli TAK, to jakie? Proszę określić rodzaje wewnętrznych wymagań oraz Jeśli NIE, to z jakiego powodu?
35.	Czy wdrożono zabezpieczenia fizyczne pomieszczeń, w których przetwarzane są informacje?	TAK NIE	Jeśli TAK, to jakie wewnętrzne dokumenty regulują ten zakres wymagań? Jeśli NIE, to z jakiego powodu?
36.	Czy wdrożono wewnętrzne zasady nadawania, zmiany i odbierania uprawnień w dostępie do informacji, w tym przetwarzanych w systemach i sieciach informacyjnych i czy wymagania te są stosowane?	TAK NIE	Jeśli TAK, to jakie wewnętrzne dokumenty regulują ten zakres wymagań? Jeśli NIE, to z jakiego powodu?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
37.	Czy dostęp użytkowników, administratorów i serwisantów do systemów informacyjnych wymaga stosowania przez nich procesu uwierzytelnienia?	TAK NIE	Jeśli TAK, to jakie wewnętrzne dokumenty regulują ten zakres wymagań oraz jakie metody uwierzytelnienia zastosowano w systemach informacyjnych? Jeśli NIE, to z jakiego powodu?
38.	Czy środki przetwarzania informacji są inwentaryzowane i odpowiednio przydzielane oraz czy są opracowane wewnętrzne wymagania w tym zakresie?	TAK NIE	Jeśli TAK, to kto jest za to odpowiedzialny (funkcja / rodzaje stanowisk) i jakie wewnętrzne wymagania regulacyjne określają ten zakres działania? Jeśli NIE, to z jakiego powodu?
39.	Czy wdrożona jest i stosowana tzw. „polityka czystego biurka”?	TAK NIE	Jeśli TAK, to w jaki sposób polityka ta jest realizowana? Jeśli NIE, to z jakiego powodu?
40.	Czy wdrożona jest i stosowana tzw. „polityka czystego ekranu”?	TAK NIE	Jeśli TAK, to w jaki sposób polityka ta jest realizowana? Jeśli NIE, to z jakiego powodu?
41.	Czy określone są wymagania i wykonywane jest szacowanie i postępowanie z ryzykiem w bezpieczeństwie informacji, w tym w ochronie danych osobowych?	TAK NIE	Jeśli TAK, to jakie wewnętrzne dokumenty regulują ten zakres wymagań? Jeśli TAK, to kiedy były przeprowadzane trzy ostatnie? MM.RRRR MM.RRRR MM.RRRR Jeśli NIE, to z jakiego powodu?
42.	Czy zawierane i realizowane są umowy wsparcia technicznego określające akceptowalne poziomy świadczonej usług serwisowych (SLA) dla systemów informatycznych, które mają być wykorzystywane do planowanego przetwarzania?	TAK NIE	Jeśli TAK, Opis nie jest wymagany. Jeśli NIE, to z jakiego powodu?
43.	Czy utrzymywany jest lub będzie zaprowadzony w wyniku powierzenia przetwarzania danych osobowych, rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora?	TAK NIE	Jeśli TAK, Opis nie jest wymagany? Jeśli NIE, to z jakiego powodu?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
44.	Czy outsourcing związany z przetwarzaniem informacji, w tym danych osobowych, realizowany jest, i jak, tylko przez uprzednio sprawdzone pod kątem zapewnienia bezpieczeństwa informacji podmioty zewnętrzne (podmioty przetwarzające)?	TAK NIE	Jeśli TAK, to w jaki sposób realizowana jest wstępna weryfikacja gwarancji bezpieczeństwa przetwarzania informacji i czy wdrożono, i jakie, wewnętrzne wymagania w tym zakresie. Jeśli NIE, to z jakiego powodu?
45.	Czy przeprowadzane są okresowe audyty bezpieczeństwa informacji, w tym w zakresie ochrony danych osobowych i czy też w podmiotach zewnętrznych (podmiotach przetwarzających), którym powierzono przetwarzanie informacji?	TAK NIE	Jeśli TAK, to jakie wewnętrzne dokumenty regulują ten zakres wymagań? Jeśli TAK, to kiedy były przeprowadzane trzy ostatnie? MM.RRRR MM.RRRR MM.RRRR Jeśli NIE, to z jakiego powodu?
46.	Czy niepotrzebne informacje oraz ich nośniki są niszczone i czy są wdrożone w tym zakresie wymagania wewnętrzne?	TAK NIE	Jeśli TAK, to jaki dokument wewnętrzny reguluje ten zakres wymagań? Jeśli NIE, to z jakiego powodu?
47.	Czy stosuje się szyfrowanie dysków serwerowych, kopii zapasowych i dysków zewnętrznych, również zainstalowanych w przenośnych urządzeniach komputerowych i czy wdrożone są wymagania wewnętrzne w tym zakresie?	TAK NIE	Jeśli TAK, to jakie są stosowane metody szyfrowania i jaki dokument wewnętrzny reguluje ten zakres wymagań? Jeśli NIE, to z jakiego powodu?
48.	Czy wdrożono i stosowane są wymagania wewnętrzne odnoszące się do zarządzania hasłami i innymi informacjami uwierzytelniającymi w dostępie do systemów informacyjnych?	TAK NIE	Jeśli TAK, to w jaki sposób i jaki dokument wewnętrzny reguluje ten zakres wymagań? Jeśli NIE, to z jakiego powodu?
49.	Czy wdrożono wymagania i realizowane są działania dotyczące zapewnienia ciągłości bezpieczeństwa informacji?	TAK NIE	Jeśli TAK, to czego one dotyczą i jaki dokument wewnętrzny reguluje ten zakres wymagań? Jeśli NIE, to z jakiego powodu?

Lp.	Pytanie	Odpowiedź	Opis do odpowiedzi
50.	Czy dostęp do pomieszczeń, w których planowane jest przetwarzanie informacji, w tym danych osobowych, możliwy jest dla osób innych, niż realizujących to przetwarzanie bez nadzoru (np. dla służb ochrony, konserwatorów, personelu sprzątającego pomieszczenia)?	TAK NIE	Jeśli TAK, to dla kogo i czy wdrożone oraz stosowane są i jakie wymagania wewnętrzne w tym zakresie? Jeśli NIE, Opis nie jest wymagany.
51.	Czy przy przetwarzaniu danych osobowych spełniane są wymagania „Privacy by default” oraz „Privacy by design”?	TAK NIE	Jeśli TAK, to czy wdrożone oraz stosowane są i jakie wymagania wewnętrzne w tym zakresie? Jeśli NIE, to z jakiego powodu?

Sporządził:

.....