ARKUSZ WERYFIKACYJNY
PRZEZNACZONY DLA PODMIOTU PRZETWARZAJĄCEGO

LP.	PYTANIE	ODPOWIEDŹ	UWAGI
1.	Czy wszystkie osoby zaangażowane (pracownicy, współpracownicy, etc.) w procesy przetwarzania danych osobowych, prowadzone przez podmiot przetwarzający, zostały przeszkolone lub poinstruowane z zasad przetwarzania danych osobowych wskazanych w RODO? Kiedy zostało przeprowadzone ostatnie szkolenia z tego zakresu?	☐ TAK ☐ NIE Informacje dotyczące szkoleń: …… …… ……....	
2.	Czy wszystkie osoby zaangażowane (pracownicy, współpracownicy, etc.) w procesy przetwarzania danych osobowych, prowadzone przez podmiot przetwarzający, zostały imiennie upoważnione przez podmiot przetwarzający?	☐ TAK ☐ NIE	
3.	Czy wszystkie osoby zaangażowane (pracownicy, współpracownicy, etc.) w procesy przetwarzania danych osobowych, prowadzone przez podmiot przetwarzający, zostały zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia, zarówno w trakcie zatrudnienia jak i po ustaniu zatrudnienia?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

4.	Czy podmiot przetwarzający powołał Inspektora ochrony danych?	☐ TAK ☐ NIE	
5.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?	☐ TAK ☐ NIE	
6.	Czy dane osobowe powierzone przez NCBR będą logicznie lub fizycznie oddzielone od innych danych przetwarzanych przez podmiot przetwarzający?	☐ TAK ☐ NIE	
7.	Czy w ciągu ostatniego roku były wykonywane testy bezpieczeństwa systemów informatycznych podmiotu przetwarzającego, w których przetwarzane będą dane osobowe powierzone przez NCBR?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

8.	Czy w ciągu ostatnich dwóch lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	☐ TAK ☐ NIE	
9.	Czy podmiot przetwarzający wdrożył wewnętrzną dokumentację (polityki, procedury) przetwarzania danych osobowych zgodną z RODO? Jeśli tak, proszę wskazać jaką.	☐ TAK ☐ NIE Informacje dotyczące dokumentacji: …… …… ……....	
10.	Czy podmiot przetwarzający wdrożył formalne zasady obsługi naruszeń bezpieczeństwa danych osobowych?	☐ TAK ☐ NIE	
11.	Czy u podmiotu przetwarzającego kiedykolwiek miało miejsce naruszenie ochrony danych osobowych? Jeżeli tak, proszę opisać, jakie zostały podjęte działania zaradcze i jakie skutki miało przedmiotowe naruszenie.	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

		Informacje dotyczące działań zaradczych oraz skutków naruszeń: …… …… ……....	
12.	Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? Jeśli tak, to w jaki sposób?	☐ TAK ☐ NIE Informacje dotyczące sposobu sprawdzenia podmiotów zewnętrznych/ podwykonawców: …… …… …….....	
13.	Czy dane osobowe powierzone przez NCBR będą przetwarzane przez podmiot przetwarzający lub jego podwykonawcę poza EOG (w kraju trzecim)?	☐ TAK ☐ NIE	
14.	Czy dane osobowe powierzone przez NCBR będą przetwarzane przez podmiot przetwarzający z wykorzystaniem chmury	☐ TAK	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

	obliczeniowej, innej niż chmura prywatna?	☐ NIE	
15.	Czy dane osobowe powierzone przez NCBR będą przetwarzane przez podmiot przetwarzający w celu przeprowadzania testów?	☐ TAK ☐ NIE	
16.	Czy podmiot przetwarzający stosuje fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych? Jeśli tak, proszę opisać jakie.	☐ TAK ☐ NIE Informacje dotyczące zabezpieczenia pomieszczeń oraz obszarów przetwarzania: …… …… ……....	
17.	Czy podmiot przetwarzający wdrożył regulacje w zakresie ruchu osobowo-materiałowego?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

18.	Czy podmiot przetwarzający prowadzi ewidencję gości wchodzących na teren podmiotu?	☐ TAK ☐ NIE	
19.	Czy goście mogą przebywać na terenie podmiotu przetwarzającego tylko w obecności upoważnionych pracowników?	☐ TAK ☐ NIE	
20.	Czy podmiot przetwarzający wdrożył formalne zasady zarządzania uprawnieniami w systemach IT?	☐ TAK ☐ NIE	
21.	Czy każdy pracownik/współpracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?	☐ TAK ☐ NIE	
22.	Czy wprowadzono zasady bezpiecznego korzystania z haseł przez użytkowników?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

23.	Czy systemy informatyczne wykorzystywane przez podmiot przetwarzający zapewniają wymuszanie na użytkownikach okresowej zmiany haseł oraz zmian w razie zaistniałej potrzeby?	☐ TAK ☐ NIE	
24.	Czy podmiot przetwarzający wprowadził formalne zasady bezpiecznej pracy w systemach informatycznych?	☐ TAK ☐ NIE	
25.	Czy pracownicy/współpracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów, poprzez blokadę ekranu lub w inny równoważny sposób?	☐ TAK ☐ NIE	
26.	Czy pracownicy podmiotu przetwarzającego mogą mieć zdalny dostęp do danych osobowych powierzonych przez NCBR?	☐ TAK ☐ NIE	
27.	Czy podmiot przetwarzający wprowadził zasady dotyczące bezpiecznej pracy zdalnej?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

28.	Czy przy dostępie zdalnym wymagana jest autoryzacja wieloskładnikowa (MFA)?	☐ TAK ☐ NIE	
29.	Czy podmiot przetwarzający zapewnia rozliczalność działań podejmowanych przez użytkowników systemów informatycznych, np. czy istnieje możliwość stwierdzenia, kto i kiedy modyfikował dane konkretnej osoby lub miał do nich wgląd?	☐ TAK ☐ NIE	
30.	Czy podmiot przetwarzający wdrożył zasady monitorowania systemów informatycznych, w których będą przetwarzane dane powierzone przez NCBR?	☐ TAK ☐ NIE	
31.	Czy podmiot przetwarzający wdrożył zapory sieciowe kontrolujące wymianę danych z Internetem i innymi zewnętrznymi sieciami, z uwzględnieniem filtracji ruchu wchodzącego i wychodzącego?	☐ TAK ☐ NIE	
32.	Czy podmiot przetwarzający wdrożył bezpieczne mechanizmy szyfrowania przesyłanych danych, zgodne z zaleceniami NIST SP800-131A?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

33.	Czy podmiot przetwarzający wprowadził bezpieczne (zgodne z NIST SP800-131A) mechanizmy szyfrowania danych, przechowywanych na przenośnych urządzeniach końcowych, tym laptopach?	☐ TAK ☐ NIE	
34.	Czy powierzone przez NCBR dane będą przechowywane przez podmiot przetwarzający na nośnikach przenośnych?	☐ TAK ☐ NIE	
35.	Czy podmiot przetwarzający zapewnia, że nośniki przenośne zawierające dane osobowe podlegają szyfrowaniu z wykorzystaniem mechanizmów zgodnych z NIST SP800-131A?	☐ TAK ☐ NIE	
36.	Czy zastosowano oprogramowanie antywirusowe na wszystkich stacjach wykorzystywanych przez pracowników/współpracowników podmiotu przetwarzającego?	☐ TAK ☐ NIE	
37.	Czy zastosowano oprogramowanie antywirusowe na wszystkich serwerach podmiotu przetwarzającego, na których będą przetwarzane dane osobowe powierzone przez NCBR?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

38.	Czy zastosowano inne środki techniczne zapewniające ochronę przez złośliwym oprogramowaniem? Jakie?	☐ TAK ☐ NIE Opis zastosowanych środków technicznych: …… …… ……	
39.	Czy pracownicy podmiotu przetwarzającego podlegają szkoleniom z zakresu unikania ryzyka związanego z występowaniem i działaniem złośliwego oprogramowania?	☐ TAK ☐ NIE	
40.	Czy podmiot przetwarzający wykorzystuje oprogramowanie wyłącznie zgodnie z postanowieniami warunków licencyjnych?	☐ TAK ☐ NIE	
41.	Czy podmiot przetwarzający wdrożył zasady utwardzania konfiguracji oprogramowania systemowego i aplikacyjnego?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

42.	Czy podmiot przetwarzający wdrożył zasady identyfikowania i zarządzania podatnościami w oprogramowaniu?	☐ TAK ☐ NIE	
43.	Czy podmiot przetwarzający wdrożył sformalizowany proces instalacji poprawek bezpieczeństwa dla eksploatowanego oprogramowania?	☐ TAK ☐ NIE	
44.	Czy podmiot przetwarzający wdrożył sformalizowane zasady zarządzania zmianą w systemach informatycznych, uwzględniające zapewnienie należytej ochrony danych?	☐ TAK ☐ NIE	
45.	Czy podmiot przetwarzający zapewnia nadzór nad serwisantami IT będącymi pracownikami firm zewnętrznych?	☐ TAK ☐ NIE	
46.	Czy podmiot przetwarzający zapewnił pozostawianie uszkodzonych nośników danych (zamiast oddawania ich firmie serwisowej w celu wymiany na sprawny nośnik)?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

47.	Czy podmiot przetwarzający wdrożył metody bezpiecznego usuwania danych z nośników wycofanych z eksploatacji? Jakie?	☐ TAK ☐ NIE Opis zastosowanych środków: …… …… ……	
48.	Jaki zakres oraz częstotliwość tworzenia kopii zapasowych danych przyjął podmiot przetwarzający?		
49.	Czy kopie zapasowe przechowywane są w sposób umożliwiający zapewnienie ciągłości działania?	☐ TAK ☐ NIE	
50.	Czy podmiot przetwarzający posiada zasady odtwarzania systemu po awarii?	☐ TAK ☐ NIE	
51.	Czy podmiot przetwarzający przeprowadza okresowe testy odtworzeniowe systemów informatycznych, w których będą przetwarzane dane osobowe powierzone przez NCBR? Jaka jest	☐ TAK	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

	częstotliwość powyższych testów?	☐ NIE Częstotliwość testów: …… …… ……	
52.	Czy podmiot przetwarzający wdrożył plany ciągłości działania obejmujące procesy związane z przetwarzaniem informacji powierzonych przez NCBR?	☐ TAK ☐ NIE	
53.	Czy podmiot przetwarzający przeprowadza regularnie, nie rzadziej niż raz na 12 miesięcy, testy i przeglądy planów ciągłości działania?	☐ TAK ☐ NIE	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

54.	Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą "ochrony danych w fazie projektowania" (*privacy by design*)? W jaki sposób realizowana jest ww. zasada przez podmiot przetwarzający?	☐ TAK ☐ NIE Informacje dotyczące sposobów realizacji zasady "ochrony danych w fazie projektowania" (*privacy by design*): …… …… ……....	
55.	Czy podmiot przetwarzający działa zgodnie z zasadą domyślnej ochrony danych (*privacy by default*)? W jaki sposób realizowana jest ww. zasada przez podmiot przetwarzający?	☐ TAK ☐ NIE Informacje dotyczące sposobów realizacji zasady " domyślnej ochrony danych" (*privacy by default*): …… …… ……....	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

56.	Czy podmiot przeprowadza okresowo analizę ryzyka przetwarzania danych osobowych? Jak często?	☐ TAK ☐ NIE Częstotliwość przeprowadzanej analizy ryzyka:	
57.	Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?	☐ TAK ☐ NIE	
58.	Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	☐ TAK ☐ NIE	
59.	Czy systemy informatyczne wykorzystywane przez podmiot przetwarzający do przetwarzania danych osobowych powierzonych przez NCBR zapewniają, że dla każdej osoby, której dane są przetwarzane, możliwe jest trwałe usunięcia tych danych?	☐ TAK	

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

		☐ NIE	

Oświadczenie Podmiotu przetwarzającego:

Działając w imieniu podmiotu przetwarzającego ..... działającego na zlecenie Narodowego Centrum Badań i Rozwoju w Warszawie, oświadczam, iż powyższe informacje są zgodne z prawdą. W przypadku zmiany któregokolwiek z wyżej wymienionych elementów, zobowiązuję się niezwłocznie, tj. nie później niż w terminie 7 dni, powiadomić o tym Narodowe Centrum Badań i Rozwoju w Warszawie.

_____ _____

Data **Podpis osoby uprawnionej**

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR