LISTA KONTROLNA (WERYFIKACYJNA) PODMIOTU PRZETWARZAJĄCEGO

Dane podmiotu przetwarzającego			
Firma podmiotu przetwarzającego			
NIP/REGON/KRS			
Adres siedziby			
Adres świadczenia usług dla administratora (jeżeli inny niż powyżej)			
Dane identyfikujące i kontaktowe osoby reprezentującej podmiot przetwarzający			
Pytania wstępne			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
1.	Czy podmiot przetwarzający przyjął zatwierdzony kodeks postępowania (art. 40 RODO)?		
2.	Czy podmiot przetwarzający jest certyfikowany zgodnie z zatwierdzonym mechanizmem certyfikacji (art. 42 RODO)?		
3.	Czy podmiot przetwarzający jest certyfikowany innymi certyfikatami jakości lub w myśl norm ISO? Jeżeli tak, proszę w uwagach podać jakimi i na jaki okres (do kiedy) obowiązuje certyfikacja.		
4.	Czy podmiot przetwarzający miał kontrolę, postępowanie wyjaśniające lub inne działania prowadzone przez Prezesa UODO lub inny organ nadzorczy po 2018 r. w związku z przetwarzaniem danych osobowych? **W przypadku pozytywnej odpowiedzi, prosimy w Uwagach/komentarzach wskazać co było przedmiotem działań prowadzonych przez Prezesa UODO i jakie są wyniki przeprowadzonych działań?**		
5.	Czy systemy lub inne aktywności związane z przetwarzaniem danych osobowych na polecenie Administratora powodują konieczność wysłania (transferu, przechowywania) do krajów spoza EEA?		
Organizacja wewnętrzna – osoby funkcyjne			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
6.	Czy podmiot przetwarzający powołał lub wyznaczył Inspektora Ochrony Danych (IOD)? **Jeżeli tak w uwagach proszę wskazać jego imię i nazwisko**. *Jeżeli nie – proszę przejść do pytania 9.*		
7.	Czy IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych?		

8.	Czy dane IOD zostały opublikowane na stronie podmiotu przetwarzającego? **W uwagach proszę wskazać adres strony.**		
9.	Czy podmiot przetwarzający powołał lub wyznaczył inną osobę, która zajmuje się monitorowaniem przestrzegania przepisów dotyczących przetwarzania i ochrony danych osobowych u podmiotu przetwarzającego? **Proszę wskazać jej imię i nazwisko i dane kontaktowe.**		
10.	Czy podmiot przetwarzający powołał lub wyznaczył Administratora Systemów Informatycznych (ASI) lub inną osobę, która opiekuje się infrastrukturą i siecią u podmiotu przetwarzającego z technicznego punktu widzenia?		
Zabezpieczenia organizacyjne – dokumentacja wewnętrzna			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
11.	Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie podatności i zagrożeń związanych z wykorzystywanymi przez siebie zasobami (aktywami), które będą wykorzystywane przy przetwarzaniu powierzonych danych osobowych? **Jeżeli tak, w uwagach proszę wskazać datę badania.**		
12.	Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie zagrożeń dla praw i wolności podmiotów danych w związku z powierzanymi czynnościami? **Jeżeli tak, w uwagach proszę wskazać datę badania.**		
13.	Czy podmiot przetwarzający posiada i wdrożył polityki ochrony danych osobowych, o których mowa w art. 24 ust. 2 RODO? **Jeżeli tak, w uwagach proszę je wymienić. Proszę załączyć strony polityk/instrukcji/procedur potwierdzające: datę ich wejścia w życie, akceptujące podpisy właściwych organów organizacyjnych.**		
14.	Czy podmiot przetwarzający posiada i wdrożył (w ramach innych polityk/procedur lub jako indywidualny dokument) procedury postępowania w przypadku incydentów bezpieczeństwa i naruszeń ochrony danych osobowych? **Proszę załączyć stronę polityki/instrukcji/procedury potwierdzającą: datę jej wejścia w życie, akceptujące podpisy właściwych organów organizacyjnych.**		
15.	Czy istnieją inne formalne procedury wspierające zgodne z prawem i bezpieczne przetwarzanie danych osobowych u podmiotu przetwarzającego? Czy procedury te zostały wdrożone i będą miały zastosowanie do przetwarzania powierzonych danych osobowych? Proszę je wymienić.		

16.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania?		
Zabezpieczenia organizacyjno-techniczne – upoważnienia i uprawnienia			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
17.	Czy osobom, które będą przetwarzały powierzone dane osobowe, nadano upoważnienia do przetwarzania danych?		
18.	Czy osoby, które będą przetwarzały powierzone dane osobowe, zostały przeszkolone z zakresu bezpieczeństwa informacji i danych osobowych?		
19.	Czy podmiot przetwarzający opracował i realizuje program szkoleń cyklicznych lub uzupełniających dla osób upoważnionych?		
20.	Czy osoby, które będą przetwarzały powierzone dane osobowe, zostały zobowiązane do zachowania poufności tych danych, sposobów ich przetwarzania i zabezpieczenia?		
21.	Czy podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych?		
Zabezpieczenia organizacyjne – współpraca z podwykonawcami			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
22.	Czy podmiot przetwarzający korzysta z usług podwykonawców, którym powierza do przetwarzania dane osobowe? ***Jeżeli nie – proszę przejść do pytania 26.***		
23.	Czy podmiot przetwarzający prowadzi rejestr/ewidencję podmiotów przetwarzających/dalszych podmiotów przetwarzających lub inny adekwatny dokument?		
24.	Czy podmiot przetwarzający przy wyborze swojego podwykonawcy przeprowadza działania pre audytowe, weryfikujące, czy podwykonawca spełnia wystarczające gwarancje wdrożenia odpowiednich środków zabezpieczających, aby przetwarzanie spełniało wymogi RODO i chroniło podmioty danych?		
25.	Czy podmiot przetwarzający przeprowadza doraźne lub bieżące audyty/kontrole swoich podwykonawców w trakcie realizacji umowy?		
Zabezpieczenia organizacyjne – zabezpieczenia fizyczne obszaru przetwarzania danych osobowych			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
26.	Czy obszar fizyczny, w ramach którego będą przetwarzane powierzone dane osobowe, został zabezpieczony przed dostępem osób nieuprawnionych?		

	Jeżeli tak, w uwagach proszę opisać, jakie zabezpieczenia fizyczne zastosowano.		
27.	Czy podmiot przetwarzający wprowadził regulacje ograniczające możliwość przebywania osób postronnych w obszarze, w którym będą przetwarzane dane osobowe?		
28.	Czy podmiot przetwarzający korzysta z usług zewnętrznych firm sprzątających/ochroniarskich lub innych, które dla realizacji swoich obowiązków muszą mieć zapewniony dostęp do obszaru przetwarzania danych osobowych? Jeżeli tak, czy dostęp tych osób do obszaru przetwarzania danych osobowych został uregulowany w sposób gwarantujący poufność przetwarzanych danych?		
29.	Czy obszar fizyczny, w którym będą przetwarzane dane osobowe, został objęty nadzorem monitoringu wizyjnego?		
30.	Czy podmiot przetwarzający opracował i wdrożył regulacje dotyczące prowadzenia monitoringu wizyjnego w obiekcie?		
31.	Czy obszar fizyczny, w którym będą przetwarzane dane osobowe, został objęty systemem alarmowym?		
32.	Czy obszar fizyczny, w którym będą przetwarzane dane osobowe, został wyposażony w systemy przeciwpożarowe?		
Zabezpieczenia organizacyjne – przechowywanie i niszczenie nośników danych			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
33.	Czy podmiot przetwarzający opracował i wdrożył zasady bezpiecznego przechowywania nośników danych osobowych (w tym nośników papierowych/tradycyjnych i nośników pamięci elektronicznych)?		
34.	Czy podmiot przetwarzający opracował i wdrożył zasady wykonywania, przechowywania, weryfikacji i niszczenia kopii zapasowych nośników danych (w tym nośników papierowych/tradycyjnych i nośników pamięci elektronicznych)?		
35.	Czy podmiot przetwarzający korzysta z usług wyspecjalizowanych podmiotów zajmujących się niszczeniem nośników zawierających dane poufne?		
Zabezpieczenia organizacyjno-techniczne – praca zdalna			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
36.	Czy podmiot przetwarzający dopuszcza pracowników do pracy zdalnej? ***Jeżeli nie – proszę przejść do pytania 38.***		

37.	Czy podmiot przetwarzający opracował i wdrożył środki zabezpieczające (organizacyjne, organizacyjno-techniczne, techniczne) umożliwiające prowadzenie bezpiecznej pracy zdalnej		
Zabezpieczenia organizacyjno-techniczne – korzystanie ze sprzętu i urządzeń			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
38.	Czy podmiot przetwarzający opracował i wdrożył zasady korzystania ze sprzętu służbowego udostępnianego pracownikom?		
39.	Czy podmiot przetwarzający zezwala na wynoszenie sprzętu służbowego i/lub urządzeń przydzielanych pracownikom poza obszar przetwarzania danych osobowych? ***Jeżeli nie – proszę przejść do pytania 46.***		
40.	Czy podmiot przetwarzający opracował i wdrożył zasady zabezpieczenia sprzętu służbowego i/lub urządzeń przydzielanych pracownikom wynoszonych poza obszar przetwarzania danych osobowych, w szczególności, czy zostały wdrożone zasady szyfrowania dysków pamięci takiego sprzętu/urządzeń?		
41.	Czy podmiot przetwarzający zezwala na korzystanie ze służbowego sprzętu i urządzeń przydzielanych pracownikom do celów prywatnych?		
42.	Czy podmiot przetwarzający prowadzi ewidencję wydanego sprzętu służbowego i urządzeń przydzielanych pracownikom?		
43.	Czy podmiot przetwarzający zezwala na korzystanie z pendrive'ów i urządzeń/dysków pamięci zewnętrznej przez pracowników? *Jeżeli nie – proszę przejść do pytania 46.*		
44.	Czy podmiot przetwarzający wdrożył zasady dotyczące szyfrowania pendrive'ów i urządzeń/dysków pamięci zewnętrznej wykorzystywanych przez pracowników?		
45.	Czy pracownicy mają możliwość instalacji własnego oprogramowania na urządzeniach/sprzęcie oddanym im w użytkowanie przez podmiot przetwarzający?		
Zabezpieczenia organizacyjno-techniczne – sprzęt			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
46.	Czy podmiot przetwarzający opracował i wdrożył zasady konserwacji sprzętu i urządzeń wykorzystywanych do przetwarzania danych osobowych?		
47.	Czy podmiot przetwarzający opracował i wdrożył zasady napraw w przypadku awarii lub uszkodzenia sprzętu		

	i urządzeń wykorzystywanych do przetwarzania danych osobowych?		
48.	Czy do realizacji powyższych czynności podmiot przetwarzający korzysta z usług innych wyspecjalizowanych podmiotów?		
49.	Czy podmiot przetwarzający posiada pomieszczenie specjalne o statusie serwerowni?		
50.	Czy podmiot przetwarzający korzysta z pomieszczenia serwerowni wynajmowanego od innego dostawcy? ***Jeżeli nie – proszę przejść do pytania 56****.*		
51.	Czy podmiot przetwarzający korzysta z serwerowni i serwera należącego do dostawcy zewnętrznego (właściciela powierzchni serwerowej i maszyny fizycznej)? ***Jeżeli nie – proszę przejść do pytania 56.***		
52.	Czy z dostawcami usług wskazanymi w pytaniu **50** lub **51** zawarto umowy regulujące kwestie zabezpieczenia pomieszczenia serwerowni/wynajmowanej powierzchni i serwera?		
53.	Czy podmiot przetwarzający opracował i wdrożył zasady zabezpieczenia pomieszczenia serwerowni, obejmujące zabezpieczenia środowiska serwerowni, dostępu, przeciwdziałające awarii zasilania, dostaw łącza Internet itp.?		
54.	Czy serwer został zabezpieczony przed nieuprawnioną ingerencją lub dostępem, np. z wykorzystaniem firewall? ***Jeżeli nie – proszę przejść do pytania 56****.*		
55.	Czy firewall stosowany dla zabezpieczenia serwera został indywidualnie skonfigurowany (nie są wykorzystywane ustawienia defaultowe)?		
Zabezpieczenia techniczne – oprogramowanie			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
56.	Czy system operacyjny wykorzystywany na sprzęcie/urządzeniach podmiotu przetwarzającego jest regularnie aktualizowany zgodnie z zaleceniami dostawcy systemu?		
57.	Czy podmiot przetwarzający korzysta wyłącznie z oprogramowania, dla którego posiada odpowiednie licencje, uprawniające do wykorzystania oprogramowania w celach komercyjnych?		
58.	Czy na stacjach roboczych zostało zainstalowane oprogramowanie antywirusowe? *Jeżeli nie – proszę przejść do pytania 61.*		

59.	Czy wdrożono zasady dotyczące aktualizacji oprogramowania antywirusowego i baz sygnatur wirusów?		
60.	Czy wdrożono mechanizmy pozwalające na bieżącą lub doraźną weryfikację aktualności oprogramowania antywirusowego i baz sygnatur wirusów?		
61.	Czy podmiot przetwarzający korzysta z oprogramowania antyspamowego (jako modułu wbudowanego w oprogramowanie antywirusowe lub jako oddzielnego oprogramowania)?		
62.	Czy podmiot przetwarzający korzysta z oprogramowania pozwalającego na bezpieczne przechowywanie kluczy logowania do różnych systemów przez użytkowników?		
Zabezpieczenia techniczne – sieć			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
63.	Czy podmiot przetwarzający korzysta z zapory sieciowej/firewalla dla zabezpieczenia sieci wewnętrznej? ***Jeżeli nie – proszę przejść do pytania 69.***		
64.	Czy zapora sieciowa/firewall stosowany dla zabezpieczenia sieci wewnętrznej został indywidualnie skonfigurowany (nie są wykorzystywane ustawienia defaultowe)?		
65.	Czy podmiot przetwarzający udostępnia sieć Wi-Fi dla osób nieupoważnionych (np. gości)? ***Jeżeli nie – proszę przejść do pytania 69.***		
66.	Czy oprogramowanie wykorzystywane do przetwarzania danych osobowych jest dostępne z poziomu wydzielonej sieci Wi-Fi dla osób nieupoważnionych (np. gości)?		
67.	Czy sieć wewnętrzna podmiotu przetwarzającego została zabezpieczona np. z wykorzystaniem hasła lub identyfikacji adresu MAC?		
68.	Czy podmiot przetwarzający korzysta z innych rozwiązań zabezpieczających sieć wewnętrzną przed nieuprawnioną ingerencją lub dostępem? Jeżeli tak, w uwagach proszę napisać jakich.		
69.	Czy wyznaczono osobę odpowiedzialną za obserwację ruchu sieciowego lub czy opracowano i wdrożono zasady postępowania pozwalające na wykrywanie i reagowanie w przypadków wzmożonego ruchu sieciowego?		
Zabezpieczenia organizacyjno-techniczne – poczta elektroniczna			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**

70.	Czy podmiot przetwarzający opracował i wdrożył zasady korzystania z poczty elektronicznej przez pracowników?		
71.	Czy podmiot przetwarzający zezwala pracownikom na korzystanie z poczty elektronicznej do celów prywatnych?		
Dobrowolne oświadczenia podmiotu przetwarzającego dotyczące bezpieczeństwa przetwarzania danych osobowych Administratora (nieobowiązkowe)			
Lp.			
72.			
73.			
74.			

Podpis osoby przeprowadzającej weryfikację podmiotu przetwarzającego/procesora IOD:

…… ……
Imię i nazwisko data:

Podpis osoby reprezentującej podmiot przetwarzający/procesora:

…… ……
Imię i nazwisko data