Ankieta dla podmiotu przetwarzającego (procesora)

Lp.	Pytanie	Odpowiedź	Poziom zgodności	Uwagi
1	Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych?			
2	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?			
3	Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?			
4	Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?			
5	Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?			
6	Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?			
7	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy?			
8	Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO?			
9	Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?			
10	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?			
11	Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?			
12	Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?			

13	Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany?			
14	Czy każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych?			
15	Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby?			
16	Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób?			
17	Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?			
18	Czy w organizacji jest stosowana polityka tzw. „czystego biurka"?			
19	Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?			
20	Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?			
21	Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane?			
22	Czy stosuje się szyfrowanie dysków komputerów przenośnych? - jeżeli występują urządzenia mobilne			
23	Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu? - jeżeli występują			
24	Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne? - jeżeli występują urządzenia mobilne			
25	Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? - jeżeli występują urządzenia mobilne			

26	Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?			
27	Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych?			
28	Gdzie są przechowywane kopie zapasowe?			
29	Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?			
30	Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"?			
31	Czy organizacja działa zgodnie z zasadą "privacy by default"?			
32	Czy organizacja prowadzi ocenę skutków dla ochrony danych?			
33	Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?			

POZIOM ZGODNOŚCI

■ Zgodność ■ Częściowa zgodność ■ Niezgodność