Załącznik nr 1

Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający – Ankieta badająca poziom zabezpieczeń

Lp.	PYTANIE	ODPOWIEDŹ (tak, nie, nie dotyczy, inne uwagi)
1.	Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
2.	Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
3.	Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
4.	Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
5.	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy?	
6.	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 ?	
7.	Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	

8.	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?	
9.	Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
10.	Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji?	
11.	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?	
12.	Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?	
13.	Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby?	
14.	Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób?	
15.	Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	
16.	Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka?	

17.	Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	
18.	Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach roboczych?	
19.	Czy podmiot przetwarzający korzysta wyłącznie z licencjonowanego oprogramowania i czy jest ono na bieżąco aktualizowane ?	
20.	Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych?	
21.	Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu?	
22.	Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych?	
23.	Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe?	
24.	Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
25.	Czy podmiot przetwarzający tworzy kopie zapasowe?	
26.	Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania?	
27.	Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?	
28.	Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do sprostowania danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	
29.	Czy podmiot przetwarzający był adresatem decyzji administracyjnej wydanej przez organ nadzorczy ochrony danych (UODO) lub orzeczenia sądu z zakresu prawa ochrony danych osobowych ?	

30.	Czy w podmiocie przetwarzającym funkcjonuje system zarządzania bezpieczeństwem informacji z serii norm np: PN-EN ISO/IEC 27001, 27002, 27005 lub inne.	
31.	Czy podmiot przetwarzający powołał Inspektora Ochrony Danych Osobowych ?	

.....

(data, pieczęć i podpis osoby reprezentującej podmiot przetwarzający)