|  |  |
| --- | --- |
| Podmiot przetwarzający (nazwa) |  |
| Adres |  |
| Inspektor ochrony danych  lub osoba kontaktowa wraz z  adresem e-mail i/lub numerem telefonu | *\*Nie ma obowiązku wyznaczania IOD, o ile nie zachodzi warunek z art. 37 RODO (podmiot publiczny, duża skala przetwarzania lub dane szczególnych kategorii)* |

| **Lp.** | **Wymóg dla podmiotu przetwarzającego** | **TAK** | **NIE** | **UWAGI** |
| --- | --- | --- | --- | --- |
| **1.** | Posiada wdrożoną Politykę ochrony danych osobowych lub inne akty wewnętrzne określające zasady ochrony danych osobowych, informowania Administratora o naruszeniach ochrony danych osobowych, realizacji praw podmiotów danych |  |  | Wymagane art. 24 i 32 RODO |
| **2.** | Osoby upoważnione do przetwarzania danych zobowiązane są do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy |  |  | Wymagane przez art. 29 RODO |
| **3.** | 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 |  |  | Wymagane przez art. 32 RODO |
| **4.** | Zapewnienia bezpieczeństwo danych poprzez wdrożone adekwatne środki techniczne i organizacyjne, np.: szyfrowanie, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych |  |  | Wymagane przez art. 32 RODO |
| **5.** | Zapewnienia regularne (co najmniej raz na rok) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania |  |  | Wymagane przez art. 32 RODO |
| **6.** | Posiada wdrożoną procedurę zarządzania ryzykiem |  |  | Wymagane przez art. 32 RODO |
| **7.** | Stosuje zatwierdzone kodeksy postępowania |  |  | Nie został zatwierdzony kodeks branżowy |
| **8.** | Posiada certyfikat w zakresie ochrony danych osobowych |  |  | Nie funkcjonują takie certyfikaty dla firm |
| **9.** | Posiada aktualne oprogramowania, zarówno użytkowe jak i systemowe, z wysokim poziomem odporności na cyberataki |  |  | Wymagane art. 32 RODO |
| **10.** | Zabezpiecza posiadane sieci komputerowe, zarówno przewodowe jak i bezprzewodowe, poprzez odpowiednią konfigurację urządzeń i systemów umożliwiającą blokowanie podejrzanej transmisji danych |  |  | Wymagane art. 32 RODO |
| **11.** | Zarządza dostępem zarówno do pomieszczeń jak i do systemów oraz programów komputerowych poprzez audytowalny proces nadawania, przeglądu i odbierania uprawnień oraz stosowanie bezpiecznych mechanizmów uwierzytelniania |  |  | Wymagane art. 32 RODO |
| **12.** | Używa silnego szyfrowania danych na urządzeniach przenośnych (takich jak laptopy czy smartfony) i pamięciach zewnętrznych (np. karty SD) a także silnego szyfrowania komunikacji odbywającej się przy pomocy sieci zewnętrznej Internet, o ile przenoszone lub przesyłane są dane osobowe, w których posiadanie podmiot przetwarzający wejdzie podczas realizacji powierzonych czynności |  |  | Wymagane art. 32 RODO |
| **13.** | Przechowuje kopie bezpieczeństwa posiadanych informacji w bezpiecznej lokalizacji i zabezpiecza je przed nieautoryzowanym dostępem |  |  | Wymagane art. 32 RODO |
| **14.** | Zapewnia kontrolowany sposób wprowadzania zmian w środowisku administratora, poprzedzony formalnym procesem testowym |  |  | Wymagane art. 5 i 32 RODO |
| **15.** | Zapewnienia kontrolowany sposób zarządzania cyklem życia informacji zarówno w formie elektronicznej jak i trwałej, w szczególności jej bezpieczne pozyskiwanie, przetwarzanie, przechowywanie i usuwanie |  |  | Wymagane art. 28 i 32 RODO |
| **16.** | Zapewnia nadzór nad osobami niebędącymi pracownikami podmiotu przetwarzającego, a przebywającymi w jego siedzibie, wykluczający ich dostęp do danych osobowych |  |  | Wymagane art. 29 RODO |
| **17.** | Przestrzega warunków korzystania z usług innych podmiotów przetwarzających |  |  | Wymagane art. 28 RODO |
| **18.** | Korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych |  |  | Wymagane art. 28 RODO |
| **19.** | Gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym |  |  | Wymagane art. 12-22 oraz 28 RODO |
| **20.** | Podmiot przechowuje i przetwarza dane osobowe (łączne z kopiami bezpieczeństwa) jedynie w krajach Europejskiego Obszaru Gospodarczego (EOG) |  |  | Wymagane art. 28 oraz 45-49 RODO, o ile administrator nie wyrazi zgody na transfer danych. W przypadku FinxS dane są transferowane do USA na podstawie standardowych klauzul umownych |
| **21.** | Podmiot Przetwarzający prowadzi rejestr kategorii czynności przetwarzania, zawierający wszystkie informacje wskazane  w art. 30 ust. 2 RODO |  |  | Z obowiązku są zwolnione małe podmioty, które nie przetwarzają danych na dużą skalę. |