**Załącznik nr 5 do Zapytania ofertowego BIT-BIG.25.24.2024**

**Lista kontrolna** – formularz oceny weryfikacji podmiotu przetwarzającego pod kątem spełniania wymagań bezpiecznego przetwarzania danych osobowych na potrzeby umowy **Nr BIT-BIG.25.24.2024** na **„Modernizację i zapewnienie wsparcia technicznego dla Systemu TechStep Essentials MDM.”**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Pytanie** | **Poziom zgodności:****zgodność/częściowa zgodność/nie dotyczy[[1]](#endnote-1)** | **Odpowiedź****(przedstawić opisowo)** | **Uwagi** |
| **1** | Czy osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych?  |  |  |  |
| **2** | Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem? |  |  |  |
| **3** | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |  |  |  |
| **4** | Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych taką jak opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |  |  |
| **5** | 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?  |  |  |  |
| **6** | Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |  |  |  |
| **7** | 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? |  |  |  |
| **8** | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |  |
| **9** | Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby? |  |  |  |
| **10** | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |  |  |
| **11** | Czy w organizacji jest stosowana polityka tzw. „czystego biurka”? |  |  |  |
| **12** | 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? |  |  |  |
| **13** | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?  |  |  |  |
| **14** | Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane? |  |  |  |
| **15** | Czy stosuje się szyfrowanie dysków komputerów przenośnych? |  |  |  |
| **16** | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |  |  |
| **17** | Czy w organizacji wykonuje się kopie zapasowe? |  |  |  |
| **18** | Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? |  |  |  |

1. W przypadku braku obowiązku spełniania wymagań wynikających z charakteru operacji przetwarzania, bądź z uwagi na wielkość jednostki należy wpisać „nie dotyczy”. [↑](#endnote-ref-1)