



## **WYKAZ MINIMALNYCH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, KTÓRE ZOBOWIĄZANY JEST WDROŻYĆ PROCESOR**

W celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych Danych osobowych Procesor jest zobowiązany przechowywać takie dane na zasobie odseparowanym od pozostałych zasobów danych Procesora, do którego dostęp możliwy jest wyłącznie z poziomu sieci lokalnej lub przez VPN Procesora, wyłącznie przez osoby upoważnione, które złożyły wobec Procesora oświadczenie o zachowaniu poufności.

Dodatkowo, Procesor zobowiązuje się posiadać przez cały okres Przetwarzania co najmniej następujące środki techniczne i organizacyjne:

1. Rozliczalność pracowników wykonujących prace nad Danymi poprzez udostępnienie w wewnętrznej infrastrukturze specjalnie dedykowanego systemu wirtualnego dla powyższych celów.
2. Posiadanie odpowiednich zasad dostępu do systemu opartych o mechanizmy kontroli dostępu Microsoft AD.
3. Łączenie ze środowiskiem poprzez sieć Internet wyłącznie po zestawieniu bezpiecznego połączenia w oparciu o VPN.
4. Fizyczny dostęp do serwerów, na których Przetwarzane są Dane i umieszczone systemu, o których mowa powyżej objęty jest kontrolą dostępu na poziomie zabezpieczeń fizycznych jak również organizacyjnych (np.: CCTV, karty dostępu, kontrola fizyczna).
5. Każda osoba mająca dostęp do powierzonych danych posiada imienne upoważnienie do Przetwarzania Danych.
6. Osoby uczestniczące w procesach Przetwarzania Danych są przeszkolone i posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania operacji na danych osobowych.
7. Każda osoba posiadająca upoważnienie do Przetwarzania Danych złożyła oświadczenie o zachowaniu ich w poufności.
8. Ciągłe zapewnienia poufności, integralności, dostępności i odporności systemów służących do Przetwarzania Danych oraz usług Przetwarzania.
9. Zapewnienie możliwości szybkiego przywrócenia dostępności Danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
10. Dokonywanie regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo Przetwarzania Danych.
11. Zapewnienie mechanizmów kontroli dostępu do systemu informatycznego, w którym przetwarza się dane osobowe, w taki sposób, że dostęp do tych danych byłby możliwy jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
12. Zapewnienie ochrony systemów informatycznych służących do Przetwarzania danych w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
13. Zapewnienie bezpieczeństwa Danych osobowych w systemie informatycznym przez wykonywanie kopii zapasowej zbiorów danych oraz programów służących do Przetwarzania Danych. Kopie zapasowe należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwać je niezwłocznie po ustaniu ich użyteczności.
14. Zapewnienie by urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające Dane osobowe – były zawsze zaszyfrowane, a po ich wykorzystaniu lub przeznaczeniu do likwidacji zostały trwale usunięte w sposób uniemożliwiający późniejsze ich odtworzenie – w sposób opisany w protokole zniszczenia.
15. Zapewnienie ochrony systemów informatycznych służących do Przetwarzania Danych przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
16. Zapewnienie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.