Wykaz minimalnych środków technicznych i organizacyjnych w ramach Umowa Powierzenia Przetwarzania Danych do Porozumienia SOPD

Działając na podstawie art. 32 Rozporządzenia 2016/679 w celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych danych WMCNT jest zobowiązany wdrożyć co najmniej następujące środki techniczne i organizacyjne:

1. zapewnić możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych osobowych oraz usług przetwarzania;
2. zapewnić możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
3. dokonywać regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych;
4. zapewnić mechanizmy 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;
5. zapewnić ochronę systemów informatycznych służących do przetwarzania danych osobowych, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłócenia w sieci zasilającej;
6. zapewnić bezpieczeństwo 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 usuwa się je niezwłocznie po ustaniu ich użyteczności;
7. zapewnić by urządzenia, dyski, lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji lub przekazania podmiotowi nieuprawnionemu pozbawić wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odzyskanie lub/i odczytanie;
8. zapewnić ochronę systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
9. zapewnić środki kryptograficzne ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.