



Załącznik 1

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

Decyzja wykonawcza 2021/915 w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725

Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych. Przykłady możliwych środków:

1. Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych
Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
2. Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
3. Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
4. Środki umożliwiające identyfikację i autoryzację użytkowników
5. Środki zapewniające ochronę danych w czasie ich przekazywania
6. Środki zapewniające ochronę danych w czasie ich przechowywania
7. Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe
8. Środki umożliwiające rejestrowanie zdarzeń
9. Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej
10. Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT
11. Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów
12. Środki zapewniające minimalizację danych
13. Środki zapewniające odpowiednią jakość danych
14. Środki zapewniające ograniczone zatrzymywanie danych
15. Środki zapewniające rozliczalność
16. Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania]
17. W przypadku przekazywania danych podmiotom przetwarzającym lub podprzetwarzającym należy również opisać konkretne środki techniczne i organizacyjne, jakie powinien zastosować podmiot przetwarzający lub podprzetwarzający, aby móc udzielić pomocy administratorowi.