

Wykaz środków technicznych i organizacyjnych wdrożonych przez podmiot przetwarzający

1. Środki techniczne i organizacyjne należy opisać szczegółowo, a nie w sposób ogólny. Przykłady wskazane w załączniku mają jedynie charakter wspierający, należy odpowiednio uzupełnić i określić zastosowane lub planowane środki ochrony. Wykaz środków powinien dotyczyć bezpośrednio zabezpieczeń powierzanych danych osobowych na drodze umowy.
2. Jeśli ADO lub powierzającym jest WM, MWM, ZWM lub Urząd, to za opis środków technicznych odpowiada Procesor (tj. Procesor opisuje jakie środki zastosuje w celu zapewnienia ochrony powierzonym mu danym osobowym).
3. Przy opisywaniu środków technicznych i organizacyjnych należy wziąć pod uwagę charakter, zakres, cel i kontekst przetwarzania oraz ryzyko dla praw i wolności osób fizycznych.
4. Przykłady ewentualnych środków:
  - 1) Środki dotyczące pseudonimizacji i szyfrowania danych osobowych  
(w ramach kategorii możemy opisać, czy dane są szyfrowane, jakie metody szyfrowania lub pseudonimizacji będą zastosowane, np. szyfrowanie TLS, AES256, tokenizacja, skracanie danych);
  - 2) Środki mające na celu ciągłe zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania  
(w ramach kategorii możemy opisać wszelkie zabezpieczenia mające wpływ na nieujawnianie danych osobowych, ich kompletność i prawidłowość, dostępność dla osób uprawnionych oraz odporność na ataki zewnętrzne mające na celu nieuprawniony dostęp do danych ich zmianę lub zniszczenie);
  - 3) Środki mające na celu zapewnienie zdolności szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego  
(w ramach kategorii możemy opisać, czy wykonuje się kopie zapasowe, czy kopie są testowane i przechowywane poza miejscem ich wykonywania);
  - 4) Procedury regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania  
(w ramach kategorii możemy opisać czy podmiot przetwarzający wdrożył i stosuje ww. procedury);
  - 5) Środki identyfikacji i autoryzacji użytkowników  
(w ramach kategorii możemy opisać, czy dane będą przetwarzane przez użytkowników posiadających unikalny identyfikator w systemie informatycznym oraz czy dostęp do systemu możliwy jest wyłącznie za uwierzytelnieniem: hasło, token, lub inna metoda);
  - 6) Środki ochrony danych podczas przekazywania  
(w ramach kategorii możemy opisać jakie są stosowane zabezpieczenia przy przekazywaniu danych osobowych do innych osób/podmiotów. W systemie elektronicznym: szyfrowanie, udostępnianie poprzez zabezpieczony serwer FTP; udostępnianie poprzez zabezpieczony kontener w chmurze, np. onedrive, google drive, inne. W systemie tradycyjnym: teczki na dokumenty, plombowanie, firma kurierska, operator pocztowy, torby/walizki z szyfrem, inne);
  - 7) Środki ochrony danych podczas przechowywania

(w ramach kategorii możemy opisać jakie zabezpieczenia będą stosowane podczas przechowywania danych np. zabezpieczone pomieszczenia, meble, infrastruktura IT);

8) Środki mające na celu zapewnienie bezpieczeństwa fizycznego miejsc, w których odbywa się przetwarzanie danych osobowych

(w ramach kategorii możemy opisać jakie będą zabezpieczenia fizyczne w obszarze przetwarzania powierzonych danych osobowych będą stosowane np. utworzenie stref dostępu, zamykanie pomieszczeń na klucz/zamek elektroniczny z ewidencją dostępu/inne oraz w jaki sposób miejsca przetwarzania będą zabezpieczone przed niekorzystnymi warunkami środowiskowymi np. nadmierna wilgotnością, pożarem, zalaniem itp.);

9) Środki mające na celu zapewnienie ewidencji zdarzeń

(w ramach kategorii możemy opisać w jaki sposób ewidencjonuje się operacje wykonywane na danych tj. utrzymuje zapisy z logów systemowych, dzienników zdarzeń dla zapewnienia rozliczalności wykonywanych operacji na danych, w tym informacji o tym, kto te operacje wykonał);

10) Środki mające na celu zapewnienie konfiguracji systemu, w tym konfiguracji domyślnej

(w ramach kategorii możemy opisać jaką dokumentację dotyczącą konfiguracji systemu informatycznego posiada Procesor, czy stosuje domyślne konfiguracje systemu np. dla konkretnych ról użytkowników itp.);

11) Środki wewnętrznego zarządzania i kierowania w zakresie technologii informacji i bezpieczeństwa informatycznego

(w ramach kategorii możemy opisać jakie udokumentowane procedury opracowano i wdrożono w zakresie bezpieczeństwa przetwarzania danych osobowych np. Polityki bezpieczeństwa informacji/danych osobowych; Procedury operacyjne np. uwierzytelniania; zarządzania uprawnieniami użytkowników, kopii zapasowych; zgłaszania naruszeń itp.);

12) Środki certyfikacji/zapewnienia procesów i produktów

(w ramach kategorii możemy opisać jakie w organizacji wdrożono formalne systemy bezpieczeństwa informacji np. ISO 27001, ISO 22301 lub inne np. zatwierdzone kodeksy postępowania, o których mowa w art. 40 RODO);

13) Środki mające na celu zapewnienie minimalizacji danych

(w ramach kategorii możemy opisać jakie procedury w zakresie minimalizacji danych tj. zapewnienia przetwarzania danych wyłącznie niezbędnych do procesu przetwarzania zostały wdrożone);

14) Środki mające na celu zapewnienie jakości danych

(w ramach kategorii możemy opisać jakie wdrożono rozwiązania gwarantujące zapewnienie odpowiedniej jakości danych tj., że te dane są prawdziwe i poprawne np. ich walidację przed wprowadzeniem do systemu);

15) Środki mające na celu zapewnienie ograniczonego zatrzymywania danych

(w ramach kategorii możemy opisać jakie narzędzia zagwarantują realizację prawa do ograniczenia przetwarzania danych);

16) Środki mające na celu zapewnienie odpowiedzialności

Załącznik nr 8 do Zapytania Ofertowego

(w ramach kategorii możemy opisać jakie wdrożono zabezpieczenia w zakresie odpowiedzialności użytkowników za przetwarzanie danych np. umowy o zachowaniu poufności "NDA");

17) Środki mające na celu umożliwienie przenoszenia danych

(w ramach kategorii możemy opisać jakie narzędzia zagwarantują realizację prawa do przenoszenia danych);

18) Środki mające na celu zapewnienie usuwania danych

(w ramach kategorii możemy opisać jakie będą stosowane metody niszczenia danych/nośników).