Załącznik nr 10

 do warunków technicznych

**Wyciąg z Polityki bezpieczeństwa
dot. współpracy z podmiotami zewnętrznymi**

## V.9 Współpraca z podmiotami zewnętrznymi.

1. W celu utrzymania bezpieczeństwa przetwarzanych w Zarządzie informacji oraz zapewnienia stosowania środków ochrony przez podmioty zewnętrzne, w zakresie udostępnionej przez Zarząd informacji lub środków komunikacji, za pomocą których zarządzają lub przetwarzają w/w informację, określono zasady dostępu podmiotów zewnętrznych do informacji oraz zasobów przeznaczonych do ich przetwarzania, a w szczególności:
2. zasady dostępu fizycznego do strefy chronionej przetwarzania danych, w tym miejsc przechowywania i przetwarzania danych;
3. zasady dostępu do Systemu Informatycznego Zarządu, w tym aplikacji i baz danych;
4. zasady dostępu do zasobów, w tym Systemu Informatycznego Zarządu.
5. Zasady, procedury oraz zakres odpowiedzialności w zakresie współpracy z podmiotami zewnętrznymi zostały określono w rozdziale V.9.3 PBI.
6. Udostępnienie lub powierzenie danych podmiotom zewnętrznym jest realizowane na podstawie umów lub porozumień.
7. Umowy/porozumienia, na podstawie których powierza się lub udostępnia dane osobowe winny zawierać informacje dotyczące:
8. czasu trwania umowy;
9. sposobu i miejsca realizacji umowy;
10. nazwy udostępnionego/ powierzonego zbioru danych osobowych;
11. zakresu i celu powierzenia/udostępnienia danych osobowych;
12. zapisów dotyczących wymagań zapewnienia środków technicznych i organizacyjnych dla zapewnienia ochrony danych osobowych - w przypadku powierzenia przetwarzania danych na podstawie rt.31 Ustawy;
13. sposobu przekazania danych w przypadku wydania danych poza obszar chroniony;
14. danych kontaktowych Administratora Bezpieczeństwa Informacji nadzorującego ochronę danych;
15. listy osób wyznaczonych/upoważnionych do przetwarzania danych w związku z realizacją umowy;
16. sposobu postępowania w przypadku naruszenia bezpieczeństwa przetwarzanych danych;
17. zobowiązania o zachowaniu w poufności przetwarzanych danych w czasie realizacji umowy i po jej zakończeniu oraz zobowiązanie do zwrotu lub zniszczenia danych po zakończeniu realizacji umowy.
18. Realizacja umowy/porozumienia na przetwarzanie zdalne odbywa się na zasadach określonych w rozdziale V.9.2. PBI.
19. W przypadku, gdy umowa/porozumienie będzie realizowane w siedzibie Zarządu na sprzęcie podmiotu zewnętrznego, porozumieniu z Działem Informatyki należy określić na piśmie wymagania dotyczące:
20. konfiguracji sprzętu – wymogów technicznych sprzętu;
21. systemu operacyjnego;
22. wymagań dotyczących oprogramowania do przetwarzania danych.
23. Procedury dotyczące instalacji i dezinstalacji sprzętu dostarczonego przez podmiot zewnętrzny i oprogramowania, określono w rozdziale III.5 Instrukcji Zarządzania SI.
24. Usługi stanowiące zasób niematerialny są świadczone na podstawie zawartych przez Zarząd umów z podmiotami zewnętrznymi i nadzorowane przez:
25. Dział Administracyjno-Techniczny – w zakresie umów na dostawę mediów tj. prąd, woda, ogrzewanie;
26. Dział Informatyki – w zakresie umów na obsługę transmisji i prezentacji danych;
27. ABI – w zakresie bezpieczeństwa przetwarzania danych osobowych oraz zgodności przetwarzania
z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami.

### V.9.1 Środki ochrony związane z działaniami podmiotów zewnętrznych

1. Osoby odpowiedzialne za współpracę z podmiotami zewnętrznymi są zobowiązane do przedłożenia projektu umowy/porozumienia z:
2. ABI – w zakresie przetwarzania danych;
3. Głównym Informatykiem – w zakresie sposobu realizacji pod kątem informatycznym.

oraz przekazywanie do Głównego Informatyka i ABI kopii zawartych umów/porozumień.

1. W umowach/porozumieniach muszą być zawarte klauzule związane z ochroną danych przetwarzanych w Zarządzie, w tym:
2. zapewnienia środków technicznych i organizacyjnych przewidzianych w Ustawie w celu zabezpieczenia przetwarzania powierzonych danych osobowych;
3. zobowiązanie do zachowania w poufności wszystkich informacji, w tym danych osobowych pozyskanych dla potrzeb realizacji umowy i po jej zakończeniu;
4. zobowiązanie do zniszczenia lub zwrotu powierzonych danych po zakończeniu trwania umowy/porozumienia;
5. reguły postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa.
6. Wszystkie osoby wskazane do realizacji umowy/porozumienia na przetwarzanie danych osobowych Zarządu muszą posiadać imienne upoważnienia wydane przez AD – zasady wydawania upoważnień określono w Zarządzeniu ODO.
7. Wydanie kluczy do pomieszczeń znajdujących się w strefie przetwarzania danych osobowych określonym w umowie/porozumieniu, odbywa się na podstawie dostarczonej do Działu Administracyjno-Technicznego listy osób wskazanych do jej realizacji, zawierającej:
8. imię i nazwisko;
9. nr dowodu osobistego;
10. nazwę firmy (jeżeli osoba jest pracownikiem firmy trzeciej);
11. nr pomieszczenia;
12. terminu realizacji umowy/porozumienia.
13. Dostęp do pomieszczeń wskazanych w umowie/porozumieniu jest realizowany zgodnie z harmonogramem pracy Zarządu. W przypadku pracy poza wskazanym w regulaminie harmonogramem czasu pracy, osoba nadzorująca realizację umowy/porozumienia musi uzyskać zgodę Dyrektora, a po jej otrzymaniu powiadomić Dział Administracyjno-Techniczny i Dział Informatyki – w celu zapewnienia pracy w systemie SI i dostępu
do pomieszczeń.
14. Dostęp do SI nadaje AS na podstawie procedury nadawania uprawnień określonej w Instrukcji zarządzania SI.
15. Wszystkie osoby upoważnione do przetwarzania danych muszą zostać zapoznane z zapisami PBI i Instrukcji zarządzania SI, w zakresie obowiązujących w Zarządzie środków ochrony.
16. Korzystanie ze sprzętu dostarczonego przez podmiot zewnętrzny w celu realizacji umowy/porozumienia odbywa się za zgodą AS po uprzednim pisemnym zgłoszeniu przez osobę nadzorującą realizację umowy/porozumienia do Działu Informatyki:
17. miejsca podłączenia sprzętu;
18. zakresu aplikacji jakie mają zostać zainstalowane na dostarczonym sprzęcie w związku z realizacją umowy/porozumienia;
19. podania konta administracyjnego w celu podłączenia sprzętu do SI Zarządu.
20. Warunkiem koniecznym do uzyskania zgody na podłączenie sprzętu do SI Zarządu jest posiadanie aktualnego:
21. systemu operacyjnego – ustalonego z Działem Informatyki;
22. systemu antywirusowego lub zgoda na zainstalowanie takiego systemu przez pracowników Działu Informatyki.
23. Instalacji i dezinstalacji sprzętu i oprogramowania dokonują pracownicy Działu Informatyki.
24. Osoba wskazana w umowie/porozumieniu do nadzoru nad jej realizacją jest zobowiązana powiadamiać o zmianach i zakończeniu realizacji umowy/porozumienia w zakresie:
25. dostępu pomieszczeń – Dział Administracyjno-Techniczny, ABI;
26. zmiany osób wskazanych do jej realizacji - Dział Informatyki, Dział Administracyjno-Techniczny, Dział Organizacyjny, ABI;
27. dostępu do SI – Dział Informatyki i ABI;
28. instalacji i dezinstalacji sprzętu dostarczonego przez wykonawcę – Dział Informatyki i ABI;
29. zmiany warunków pracy zdalnej – Dział Informatyki i ABI.

### V.9.2 Środki ochrony związane z pracą zdalną podmiotów zewnętrznych

1. Umowa/porozumienie na pracę zdalną z podmiotem zewnętrznym, musi zawierać zapisy określające zasady:
2. dostępu, w tym:
3. konfiguracji dostępu – kont dostępowych, dostępnych portów i usług,
4. dni i godzin realizowania dostępu,
5. kontroli sesji zdalnej;
6. nadzoru nad realizacją umowy;
7. odpowiedzialności Zarządu za realizację umowy, w tym zapewnienie:
8. działania systemów i urządzeń transmisji danych,
9. dostępu do zasobów niezbędnych do realizacji zawartej umowy/porozumienia;
10. odpowiedzialności podmiotu zewnętrznego, w tym osób realizujących umowę/porozumienie; w zakresie zachowania:
11. poufności przetwarzanych danych,
12. tajemnicy sposobu zabezpieczenia danych i dostępu,
13. poufności sprzętu na którym będzie realizowany dostęp zdalny – zapewnienie, że dostęp do sprzętu posiadają wyłącznie upoważnione osoby;
14. powiadamiania i odpowiedzialności za wystąpienie incydentu naruszenia bezpieczeństwa.
15. Zapewnienie dostępu do SI Zarządu oraz zasobów realizuje AS, na wniosek osoby odpowiedzialnej za realizację umowy/porozumienia na zasadach określonych w umowie/porozumieniu, zgodnie z procedurą określoną w Instrukcji zarządzania SI.

### V.9.3Odpowiedzialność związana z działaniem podmiotów zewnętrznych

1. Osoba wyznaczona przez Zarząd do nadzoru realizacji umowy/porozumienia, odpowiada za:
2. pozyskanie od osób wskazanych do realizacji umowy/porozumienia danych, niezbędnych do sporządzenia wniosku, o którym mowa w pkt. 2 oraz podpisanych oświadczeń o zachowaniu w tajemnicy danych zawartych w zbiorach danych osobowych pozyskanych w trakcie realizacji umowy i po jej zakończeniu oraz sposobu zabezpieczenia danych;
3. wypełnienie dostępnego w aplikacji Mdok „Wniosku o udzielenie/odwołanie upoważnienia
do przetwarzania ZDO” i przekazanie go do Działu Organizacyjnego, w celu przygotowania imiennego upoważnienia do przetwarzania danych osobowych wskazanych w treści wniosku zbiorów danych osobowych;
4. w przypadku przetwarzania danych osobowych powierzonych zgodnie z art. 31 Ustawy, w wyniku zawartej przez Zarząd umowy/porozumienia – uzyskania listy osób upoważnionych przez podmiot zewnętrzny wskazany w umowie/porozumieniu do przetwarzania danych w powierzonym zbiorze danych osobowych;
5. wystąpienie z wnioskiem do Działu Informatyki o dostęp do aplikacji i zasobów SI Zarządu
dla upoważnionych pracowników podmiotów zewnętrznych – jeśli dostęp jest niezbędny dla realizacji umowy/porozumienia;
6. zapewnienie zapoznania osób upoważnionych wskazanych do realizacji umowy/porozumienia
z zasadami i procedurami obowiązującymi w Zarządzie w zakresie ochrony przetwarzania danych osobowych obowiązujących w Zarządzie;
7. dostarczenie do Działu Administracyjno-Technicznego listy osób realizujących umowę/porozumienie
w siedzibie Zarządu, z podaniem:
8. imienia i nazwiska,
9. numery dowodu osobistego,
10. numeru pomieszczenia, w którym będzie realizowana umowa (w celu wydania klucza),
11. harmonogramu pracy z podaniem dni i godzin;
12. jeśli realizacja umowy odbywa się na sprzęcie dostarczonym przez podmiot zewnętrzny realizujący umowę/porozumienie – powiadomienie Działu Informatyki (NGI) i ABI zgodnie z zapisami rozdziału V.9 pkt.6 PBI;
13. przestrzeganie zapisów umowy w zakresie :
14. sposobu i miejsca przetwarzania,
15. aktualizacji upoważnień dla osób realizujących umowę,
16. przestrzegania harmonogramu pracy,
17. korzystania ze sprzętu komputerowego;
18. zgłaszanie ABI incydentów naruszenia bezpieczeństwa związanych z realizacją umowy/porozumienia, również tych zgłaszanych przez osoby realizujące umowę/porozumienie, zgodnie procedurą określoną
w „Instrukcji postępowania z incydentami”.
19. Pracownicy podmiotu zewnętrznego wskazani do realizacji umowy/porozumienia, odpowiadają za:
20. zachowanie w poufności danych pozyskanych w trakcie trwania umowy/porozumienia i po jej zakończeniu oraz sposobu zabezpieczenia danych;
21. przestrzegania obowiązujących w Zarządzie zasad i procedur dotyczących ochrony przetwarzania danych;
22. zgłaszanie osobie wyznaczonej przez Zarząd do nadzoru realizacji umowy/porozumienia, zdarzeń naruszających bezpieczeństwo przetwarzania danych lub łamiące obowiązujące w Zarządzie zasady i procedury;
23. wykorzystanie sprzętu, aplikacji i danych wyłącznie w zakresie przewidzianym w umowie/porozumieniu;
24. jeśli realizacja umowy odbywa się zdalnie za pomocą łączy teleinformatycznych, realizujący umowę/porozumienie, odpowiada za:
25. zachowanie w poufności sprzętu na którym realizowany jest dostęp zdalny - zapewnienie dostępu do sprzętu wyłącznie osobom realizującym umowę,
26. zapewnienie środków ochrony przed nieuprawnionym dostępem, kradzieżą lub modyfikacją danych oraz zabezpieczenie przed działaniem szkodliwego oprogramowania,
27. zachowanie zachowania w poufności zastosowanych środków ochrony i sposobu dostępu.
28. Dział Organizacyjny odpowiada za wydanie, aktualizację i odwołanie upoważnień do przetwarzania danych osobowych na podstawie wniosku osoby nadzorującej umowę/porozumienie.
29. Dział Informatyki odpowiada za instalację i dezinstalację sprzętu i oprogramowania na podstawie pisemnej informacji pozyskanej od osoby nadzorującej realizację umowy/porozumienia, a w przypadku umowy/porozumienia realizowanego zdalnie, odpowiada za:
30. przydzielenie i odebranie dostępu do zasobów i usług określonych w umowie/porozumieniu,
31. nadzorowanie sesji zdalnej przez kontrolę czasu trwania sesji, miejsca nawiązania sesji (IP źródła), użytkownika zestawiającego sesję, zasobu z którym nawiązano połączenie podczas sesji zdalnej
– monitorowanie logów systemowych.
32. AS odpowiada za nadanie i odebranie uprawnień dostępu do zasobów SI Zarządu osobom upoważnionym, realizującym umowę/porozumienie. Nadanie uprawnień lub przedłużenie odbywa się zgodnie z procedurą określoną w Instrukcji zarządzania SI.
33. Poszczególni AOU odpowiadają za nadawanie i odbieranie uprawnień dostępu do aplikacji w Systemie SI dla osób upoważnionych wskazanych do realizacji umowy/porozumienia, w zakresie zgodnym z pisemnym wnioskiem osoby nadzorującej jej realizacje.