

Informacja kontrolach przeprowadzonych przez Urząd

Nazwa jednostki kontrolowanej:	Stowarzyszenie Białostockiego Obszaru Funkcjonalnego, pełniące funkcję Instytucji Pośredniczącej Zintegrowane Inwestycje Terytorialne Białostockiego Obszaru Funkcjonalnego (IP ZIT BOF)
Numer sprawy zgodny z Jednolitym Rzeczym Wykazem Akt Organów Samorządu Województwa i Urzędów Marszałkowskich:	DRR-XI.44.12.2020
Numer umowy/decyzji o dofinansowanie ze środków UE lub budżetowych:	<i>Porozumienie w sprawie powierzenia Instytucji Pośredniczącej zadań dotyczących realizacji Zintegrowanych Inwestycji Terytorialnych w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2014-2020 oraz wdrażania Strategii Zintegrowanych Inwestycji Terytorialnych Białostockiego Obszaru Funkcjonalnego (Porozumienie) z dnia 20 lipca 2015 r. z późn. zm., zawarte pomiędzy Zarządem Województwa Podlaskiego a Stowarzyszeniem Białostockiego Obszaru Funkcjonalnego</i>
Tytuł projektu/nazwa zadania podlegającego kontroli:	Zgodnie z planem kontroli systemowych w Rocznym Planie Kontroli realizowanym w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2014-2020 na rok obrachunkowy od 1 lipca 2020 r. do 30 czerwca 2021 r. sprawdzenie prawidłowości realizacji przez IP ZIT BOF zadań w ramach RPOWP 2014-2020 powierzonych <i>Porozumieniem</i> z dnia 20 lipca 2015 r.
Miejsce i termin przeprowadzenia kontroli:	ul. Mickiewicza 74 lok. 6, 15-232 Białystok, 29.09.2020 r. – 09.11.2020 r.
Zakres /przedmiot kontroli:	<p>W toku kontroli dokonano weryfikacji poprawności stosowania procedur oraz przestrzegania przez Instytucję Pośredniczącą zapisów Porozumienia w sprawie powierzenia Instytucji Pośredniczącej zadań dotyczących realizacji Zintegrowanych Inwestycji Terytorialnych w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2014-2020 (RPOWP 2014-2020) oraz wdrażania Strategii Zintegrowanych Inwestycji Terytorialnych Obszaru Funkcjonalnego.</p> <p>Przedmiotem kontroli systemowej było uzyskanie pewności, że wszystkie powierzone ww. Porozumieniem funkcje oraz zadania są realizowane w odpowiedni sposób, a system zarządzania i kontroli RPOWP 2014-2020 funkcjonuje prawidłowo, skutecznie i zgodnie z prawem.</p> <p>Kontroli poddano:</p> <ol style="list-style-type: none">1. Realizacja zadań w zakresie naboru, oceny i wyboru do dofinansowania powierzonych zgodnie z Porozumieniem.2. Monitorowanie i sprawozdawczość z realizacji Zintegrowanych Inwestycji Terytorialnych, w tym proces monitorowania stanu przygotowania projektów pozakonkursowych oraz osiąganie celów pośrednich i końcowych.3. Realizację obowiązków w zakresie zabezpieczania i przetwarzania danych osobowych.
Ustalenia kontroli:	Zespół Kontrolujący w kontrolowanym zakresie nie stwierdził nieprawidłowości, zadania realizowane są prawidłowo zgodnie z Procedurami oraz z zawartym Porozumieniem, niemniej jednak w pewnych kwestiach potrzebne są niewielkie usprawnienia z uwagi na stwierdzone uchybienia.
Zalecenia pokontrolne:	Wydane zalecenia pokontrolne dotyczyły obszarów, w których w trakcie czynności kontrolnych stwierdzono uchybienia: a) zalecono uzupełnienie zapisów w funkcjonujących politykach Stowarzyszenia w zakresie okresowych przeglądów aktualności i adekwatności wdrożonych polityk oraz określenia odpowiednich zasad współpracy z Administratorem Systemu Informatycznego, jeśli funkcja ta będzie realizowana przez podmiot zewnętrzny.

- b) zalecono uzupełnienie zapisów w obowiązujących politykach o procedury związane z szyfrowaniem danych, zwłaszcza w zapisach backup-u oraz faktyczne ich wdrożenie na serwerze backup-u.
- c) zalecono wdrożenie proceduralnego testowania kopii bezpieczeństwa w obowiązujących politykach oraz faktycznego ich wykonywania w sposób umożliwiający dokumentowanie tej czynności (logi systemowe lub innego rodzaju dokumentowanie).
- d) zalecono wydzielenie funkcji użytkownika stacji roboczej, który nie będzie miał uprawnień administracyjnych oraz wdrożenie mechanizmów okresowej zmiany hasła na koncie administratora, które powinno być zarezerwowane dla roli ASI.
- e) zalecono unormowanie zasad przeprowadzania szkoleń w polityce ochrony danych osobowych.
- f) zalecono wypełnienie obowiązku przez Stowarzyszenie BOF wynikającego z art. 5 umowy powierzenia, tj. poinformowania i uzyskania zgody Podmiotu powierzającego na dalsze powierzenie do przetwarzania danych osobowych. Zaleca się również zawieszenie współpracy z podmiotami świadczącymi usługi na rzecz Podmiotu przetwarzającego w części związanej z przetwarzaniem danych do czasu poinformowania Podmiotu powierzającego o zawartych umowach, ich treści, sposobie zabezpieczenia danych oraz uzyskania zgody Administratora na dalsze powierzenie danych.
- g) zalecono aktualizację podstawy prawnej klauzuli informacyjnej zawartej w części VIII uproszczonego wniosku o dofinansowanie.
- h) zalecono wdrożenie mechanizmów okresowej i regularnej zmiany hasła systemowego konta administracyjnego.
- i) Zaleca się wdrożenie zabezpieczeń dostępowych do sieci z wykorzystaniem gniazdek sieciowych w siedzibie podmiotu, poprzez wdrożenie mechanizmów atentujących (np. mac adresów stacji roboczych).
- j) zalecono wprowadzenie rozwiązania polegającego na automatycznym skanowaniu podłączonych zewnętrznych nośników informacji przez program antywirusowy, przed ich otwarciem. Komputery wykorzystywane poza siedzibą Stowarzyszenia (laptopy) muszą mieć zaszyfrowane systemowo dyski twarde, a dostęp do konfiguracji urządzenia z poziomu BIOS musi być zabezpieczony hasłem.
- k) zalecono wdrożenie ograniczeń na kontach użytkowników. Konto administracyjne powinno być wykorzystywane jedynie do zadań konfiguracyjnych stacji roboczej.
- l) zalecono wdrożenie mechanizmów umożliwiających odtwarzanie aktywności sieciowej np. poprzez historię przeglądarki.
- m) zalecono zwiększenie bezpieczeństwa osobowego przy zarządzaniu infrastrukturą informatyczną.
- n) zalecono sformalizowanie sposobu zarządzania kluczami poprzez wprowadzenie polityki zarządzania dostępem do pomieszczeń.
- o) zalecono sformalizowanie polityki czystego biurka poprzez zapisy w politykach bezpieczeństwa.
- p) zalecono sformalizowanie w polityce bezpieczeństwa zasad korzystania z elektronicznych nośników danych.
- q) zalecono uzupełnienie polityki bezpieczeństwa systemów informatycznych o regulacje dotyczące ciągłości działania.

W piśmie znak BZ-BOF-I-21-2020 z dnia 08.02.2021 r. IP ZIT BOF zobowiązała się do wdrożenia zaleceń/rekomendacji, wskazując jednocześnie sposób ich wdrożenia.

W piśmie znak DRR-XI.44.12.2020 r. z 23.02.2021 r. IZ RPOWP zaakceptowała zadeklarowany przez IP ZIT BOF sposób wdrażania zaleceń pokontrolnych, z wyjątkiem jednego zaproponowanego przez IP ZIT BOF, którego to sposobu nie

	<p>zaakceptowała.</p> <p>Pismem znak BZ-BOF-I-21-2020 z dnia 08.03.2021 r. IP ZIT BOF przekazała informacje o częściowym wykonaniu zaleceń oraz przedłożyła kopie zaktualizowanych dokumentów.</p> <p>IZ RPOWP pismem znak DRR-XI.44.12.2020 r. z 17.03.2021 r. zaakceptowała wdrożone przez IP ZIT BOF zalecenia dotyczące uzupełnienia/aktualizacji zapisów w politykach ochrony danych osobowych i poinformowała jednostkę kontrolowaną, że pozostałe zalecenia zostaną zweryfikowane podczas kolejnej kontroli systemowej w IP ZIT BOF.</p>
Akta sprawy:	<ul style="list-style-type: none"> – upoważnienie do przeprowadzania kontroli, – pismo zawiadamiające o podjęciu czynności kontrolnych, – korespondencja z jednostką kontrolowaną, – Informacja pokontrolna – Lista sprawdzająca wraz z załącznikami.
Osoby przeprowadzające kontrolę:	<ol style="list-style-type: none"> 1. Pani Wiesława Kulesza – Kierownik Zespołu Kontrolującego 2. Pani Magdalena Romanowska – Członek Zespołu Kontrolującego 3. Pan Robert Kursa – Członek Zespołu Kontrolującego 4. Pan Tomasz Kawrygo – Członek Zespołu Kontrolującego
Opracował informację:	Wiesława Kulesza, główny specjalista w Departamencie Rozwoju Regionalnego UMWP
Data opracowania:	07.04.2021 r.
Dokumenty związane z kontrolą dostępne są w godzinach pracy Urzędu w :	Urząd Marszałkowski Województwa Podlaskiego Departament Rozwoju Regionalnego ul. Poleska 89, 15-874 Białystok