ANKIETA DLA PODMIOTU PRZETWARZAJĄCEGO	
Nazwa i numer postępowania	Świadczenie usług infolinii Systemu iPFRON+ oraz SOW (numer postępowania: ZP/34/23)
Zamawiający	**Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych**
Wykonawca wypełniający ankietę	Należy podać firmę i adres Wykonawcy
Pytanie	**Odpowiedź wraz z uzasadnieniem**
Czy wprowadzona została polityka ochrony danych osobowych lub inne akty wewnętrzne regulujące zasady przetwarzania danych osobowych, w tym ich udostępniania, powierzania, retencji, obsługi wniosków podmiotów danych?	Proszę wskazać, jakie akty, np. zarządzenia, uchwały, regulaminy, procedury, zbiory najlepszych praktyk, wraz z ich nazwą, numerem i datą wydania (o ile posiadają), regulują te kwestie.
Czy polityka ochrony danych osobowych lub inny równoważny akt wewnętrzny podlegają okresowym przeglądom, w szczególności w zakresie zgodności z obowiązującymi przepisami, decyzjami i wytycznymi organów nadzorczych lub orzeczeniami sądów?	Tak / Nie W przypadku odpowiedzi "Tak" proszę wskazać, kiedy był przeprowadzany ostatni przegląd tej dokumentacji.
Czy w związku ze współpracą z PFRON prowadzony będzie rejestr kategorii czynności przetwarzania?	Tak / Nie W przypadku odpowiedzi "Nie" proszę uzasadnić swoje stanowisko.
Czy wdrożone zostały mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych?	Proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy prowadzony jest rejestr naruszeń?	Tak / Nie
Czy w ciągu ostatnich 6 miesięcy doszło do naruszenia ochrony danych osobowych podlegającego zgłoszeniu organowi nadzorczemu?	Tak / Nie

Czy podmiot przetwarzający posiada certyfikaty lub wdrożył normy w zakresie bezpieczeństwa informacji lub wdrożył system zarządzania bezpieczeństwem informacji?	Tak / Nie. W przypadku odpowiedzi "Tak", proszę wskazać, jakie są to certyfikaty.
Czy został powołany inspektor ochrony danych?	Tak / Nie W przypadku odpowiedzi "Nie", proszę wskazać, dlaczego nie został powołany i czy była przeprowadzona analiza konieczności powołania inspektora ochrony danych?
Czy w przypadku niepowołania inspektora ochrony danych została wyznaczona osoba do wykonywania zadań związanych z zapewnieniem zgodności z prawem przetwarzania danych osobowych ?	Tak / Nie W przypadku odpowiedzi "Nie", proszę wskazać, kto odpowiada za bieżacą obsługę spraw dotyczących ochrony danych ososbowych.
Czy inspektor ochrony danych lub osoba wyznaczona do wykonywania zadań związanych z zapewnieniem zgodności z prawem przetwarzania danych osobowych posiada niezbędne kwalifikacje zawodowe, w tym fachową wiedzę w zakresie prawa i praktyki stosowania przepisów o ochronie danych osobowych?	Tak / Nie
Czy dostęp do powierzanych danych osobowych zapewniony jest wyłącznie osobom do tego upoważnionym?	Tak / Nie
Czy osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania ich w tajemnicy także po zakończeniu współpracy z podmiotem przetwarzającym lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?	Tak / Nie
Czy osoby upoważnione do przetwarzania danych zostały przed otrzymaniem upoważnienia przeszkolone z ochrony danych osobowych, w szczególności, czy zostały im przedstawione obowiązujące w tym zakresie przepisy oraz wewnętrzne akty wydane przezd podmiot przetwarzający?	Tak / Nie

Czy osoby upoważnione do przetwarzania danych uczestniczą w okresowych, nie rzadziej niż raz w roku, szkoleniach z zakresu ochrony danych osobowych oraz zasad bezpiecznego korzystania z systemów informatycznych i użytkowania urządzeń, z wykorzystaniem których przetwarzane są dane osobowe?	Tak / Nie
Czy udział w szkoleniach jest dokumentowany?	Tak / Nie W przypadku odpowiedzi "Nie", proszę wskazać, jak podmiot przetwarzający wykaże realizację szkoleń zgodnie z art.. 5 ust. 2 RODO.
Czy prowadzony jest rejestr osób upoważnionych do przetwarzania danych osobowych lub w inny sposób zapewnione jest monitorowanie dostępu do danych osobowych?	Tak / Nie W przypadku odpowiedzi "Nie" proszę wskazać, z jakich przyczyn nie jest monitorowany dostęp do danych osobowych.
Czy przed wdrożeniem nowych rozwiązań uwzględniona jest zasada ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych?	Tak / Nie W przypadku odpowiedzi "Tak" proszę o wskazanie, gdzie (np. w jakim dokumencie) jest uregulowany sposób realizacji tych zasad. W przypadku odpowiedzi "Nie" proszę wskazać, z jakich przyczyn zasady te nie są realizowane.
Czy prowadzona jest analiza ryzyka naruszenia praw i wolności osób fizycznych?	Tak / Nie W przypadku odpowiedzi "Nie" proszę wskazać, z jakich przyczyn nie jest prowadzona analiza ryzyka.
Czy okresowo dokonywany jest przegląd ryzyk związanych z przetawrzaniem danych ososbowych?	Tak / Nie W przypadku odpowiedzi "Tak" proszę wskazać, kiedy był przeprowadzany ostatni przegląd ryzyk. W przypadku odpowiedzi "Nie" proszę wskazać, z jakich przyczyn przegląd nie jest przeprowadzany.
Czy w związku z planowanym zawarciem umowy powierzenia z PFRON konieczne było aktualizacja analizy ryzyka?	Tak / Nie
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy zarządzania incydentami IT?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.

Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy zarządzania uprawnieniami w systemach IT?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy zarządzania podatnościami?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy zarządzania bezpieczeństwem infrastruktury teleinformatrycznej, w szczególności systemów operacyjnych, systemów aplikacyjncyh, WAF, DAF, IPS, DLP, disaster recovery plan, korzystania z ochrony AntiVirus i AntiMalware, SIEM?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy tworzenia kopii zapasowych?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy korzystania z urządzeń mobilnych (MDM)?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy dotyczące eksploatacji środowisk wirtualnych?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy dotyczące bezpieczeństwa poczty elektronicznej?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy bezpieczeństwa sieci Wi-Fi?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy zarządzania ciągłością działania?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.

Czy podmiot przetwarzający procedury odtwarzania systemu po awarii oraz procedury i testowania?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy capacity management?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy bezpieczeństwa fizycznego i środowiskowego?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/system ruchu osobowo-materiałowego?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy dostęp do pomieszczeń stanowiących obszary przetwarzania danych osobowych jest możliwy poza godzinami pracy dla osób trzecich (np. firma sprzątająca, pracownicy ochrony)?	Tak / Nie W przypadku odpowiedzi "Tak" proszę o wskazanie kategorii osób trzecich oraz czy dostęp jest nadzorowany przez podmiot przetwarzający.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy dla technicznych systemów bezpieczeństwa, takich jak system sygnalizacji włamania i napadu, system kontroli dostępu, system telewizji przemysłowej?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy w podmiocie przetwarzającym wprowadzone zostały procedury/zasady/instrukcje/systemy wymagania dla systemów środowiskowych stosowanych dla zabezpieczenia urządzeń IT: klimatyzacji, zasilania, ochrony przeciwpożarowej, monitoringu parametrów środowiskowych?	Tak / Nie W przypadku odpowiedzi "Tak", proszę wskazać, jakie akty, np. zarządzenia, uchwały, wraz z ich nazwą, numerem i datą wydania, regulują te kwestie.
Czy podmiot przetwarzający zapewnia fizyczne lub logiczne oddzielene danych osobowych powierzonych przez PFRON od innych danych przetwarzanych przez podmiot przetwarzający?	Tak / Nie. W przypadku odpowiedzi "Nie" proszę wskazać, jakie alternatywne środki bezpieczeństwa zostały wprowadzone.

Jaki będzie stosowany mechanizm legalizujący transfer poza EOG danych osobowych powierzanych przez PFRON?	W przypadku, gdy umowa główna nie przewiduje transferu danych poza obszar EOG - proszę wpisać "Nie dotyczy". W przypadku, gdy umowa główna przewiduje transfer danych poza obszar EOG i podmiot przetwarzający będzie przetwarzał dane osobowe poza tym obszarem - proszę udzielić odpowiedzi. W przypadku, gdy umowa główna przewiduje transfer danych poza obszar EOG, ale podmiot przetwarzający nie będzie przetwarzał danych osobowych poza tym obszarem - proszę wpisać "Przedmiot umowy głównej będzie realizowany na obszarze EOG".
Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez PFRON w związku z powierzeniam danych osobowych, w tym obejmującego audyt w miejscu przetwarzania powierzonych danych osobowych lub w innym miejscu, w którym znajduje się infrastruktura lub prowadzone są prace mające wpływ na organizację i bezpieczeństwo tych danych?	Tak / Nie W przypadku odpowiedzi "Nie" proszę uzasadnić swoje stanowisko.
Jaki zakres usług objętych współpracą z PFRON zostanie podpowierzony podwykonawcom?	W przypadku, gdy umowa główna nie przewiduje podwykonawstwa - proszę wpisać "Nie dotyczy". W przypadku, gdy umowa główna przewiduje podwykonawstwo i podmiot przetwarzający będzie korzystał ze wsparcia podwykonawców - proszę udzielić odpowiedzi. W przypadku, gdy umowa główna przewiduje podwykonawstwo, ale podmiot przetwarzający nie będzie korzystał ze wsparcia podwykonawców - proszę wpisać "Przedmiot umowy głównej będzie realizowany bez wsparcia podwykonawców".

Czy podmioty podprzetwarzające są weryfikowane przed rozpoczęciem współpracy z nimi pod kątem zapewnienia zgodności z prawem i bezpieczeństwa przetwarzania danych osobowych?	W przypadku, gdy umowa główna nie przewiduje podwykonawstwa - proszę wpisać "Nie dotyczy". W przypadku, gdy umowa główna przewiduje podwykonawstwo i podmiot przetwarzający będzie korzystał ze wsparcia podwykonawców - proszę udzielić odpowiedzi. W przypadku, gdy umowa główna przewiduje podwykonawstwo, ale podmiot przetwarzający nie będzie korzystał ze wsparcia podwykonawców - proszę wpisać "Przedmiot umowy głównej będzie realizowany bez wsparcia podwykonawców".
Czy podmiot przetwarzający zawrze umowę z podmiotem podprzetwarzającym na warunkach analogicznych, jak te obowiązujące pomiędzy podmiotem przetwarzającym a PFRON?	W przypadku, gdy umowa główna nie przewiduje podwykonawstwa - proszę wpisać "Nie dotyczy". W przypadku, gdy umowa główna przewiduje podwykonawstwo i podmiot przetwarzający będzie korzystał ze wsparcia podwykonawców - proszę udzielić odpowiedzi. W przypadku, gdy umowa główna przewiduje podwykonawstwo i podmiot przetwarzający nie będzie korzystał ze wsparcia podwykonawców - proszę wpisać "Nie dotyczy".
Czy podmioty podprzetwarzające będą przetwarzać powierzane dane osobowe poza EOG?	W przypadku, gdy umowa główna nie przewiduje podwykonawstwa - proszę wpisać "Nie dotyczy". W przypadku, gdy umowa główna przewiduje podwykonawstwo i dopuszcza transfer danych poza EOG, a podmiot przetwarzający będzie korzystał ze wsparcia podwykonawców - proszę udzielić odpowiedzi. W przypadku, gdy umowa główna przewiduje podwykonawstwo i dopuszcza transfer danych poza EOG, ale podmiot przetwarzający nie będzie korzystał ze wsparcia podwykonawców - proszę wpisać "Przedmiot umowy głównej będzie realizowany bez wsparcia podwykonawców".

Czy podmiot przetwarzający prowadzi audyty lub kontrole podmiotów podprzetwarzających w zakresie ochrony danych osobowych?	W przypadku, gdy umowa główna nie przewiduje podwykonawstwa - proszę wpisać "Nie dotyczy". W przypadku, gdy umowa główna przewiduje podwykonawstwo i podmiot przetwarzający będzie korzystał ze wsparcia podwykonawców - proszę udzielić odpowiedzi. W przypadku, gdy umowa główna przewiduje podwykonawstwo, ale podmiot przetwarzający nie będzie korzystał ze wsparcia podwykonawców - proszę wpisać "Przedmiot umowy głównej będzie realizowany bez wsparcia podwykonawców".
Czy podmiot przetwarzający był poddawany zewnętrznemu audytowi niezależnych ekspertów w zakresie organizacji systemu ochrony danych osobowych?	Tak / Nie W przypadku odpowiedzi "Tak" proszę wskazać, kiedy był przeprowadzony taki audyt i czy zostały wdrożone zalecenia wynikające z audytu. W przypadku ich niewdrożenia proszę wskazać, z jakich przyczyn.
Czy podmiot przetwarzający był kontrolowany przez Prezesa Urzędu Ochrony Danych Osobowych?	Tak / Nie W przypadku odpowiedzi "Tak" proszę wskazać, kiedy odbyła się kontrola.
Czy podmiot przetwarzający zobowiązuje się do realizacji omówiązków wynikających z umowy powierzenia przetwarzania?	Tak / Nie

Potwierdzam zgodność ze stanem faktycznym przedstawionych powyżej informacji

…….

PODPIS

(ankietę należy podpisać zgodnie z reprezentacją Wykonawcy)