



PLUS HELP NGO
PROGRAM WSPARCIA ORGANIZACJI
POMOCOWYCH W POLSCE

E-BOOK WDROŻENIOWY | WERSJA 0.9

PAKIET MODELOWYCH POLITYK ORGANIZACYJNYCH DLA NGO POMOCOWYCH

ETYKA | WSPÓŁPRACA | BEZPIECZEŃSTWO

**Model minimalny możliwy do wdrożenia przez mikro-, małe i średnie
organizacje pomocowe**

Pełny przewodnik wdrożeniowy: Etyka - Współpraca - Bezpieczeństwo

Stowarzyszenie Inicjatywa Obywatelska Pro Civium | Poznań, 2026



SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM
ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU
FUNDUSZ INICJATYW OBYWATELSKICH NOWEFIO NA LATA 2021-2030

Status dokumentu: Dokument stanowi kompletny projekt pakietu trzech polityk organizacyjnych wymaganych w Działaniu 4 projektu. Po konsultacji Rady Społecznej ds. Standardów Współpracy, audycie prawnym, psychologicznym i RODO oraz pilotażu w organizacjach testowych powinien zostać oznaczony jako wersja 1.0.

Pole	Informacja
Tytuł projektu	PLUS Help NGO - Program Systemowego Wsparcia Organizacji Pomocowych w Polsce
Działanie	Standardy Współpracy NGO - Specjaliści dla Organizacji Pomocowych
Produkt	Pakiet 3 polityk organizacyjnych: Etyka, Współpraca, Bezpieczeństwo
Opracowanie	Stowarzyszenie Inicjatywa Obywatelska Pro Civium
Wersja	0.9 - projekt do konsultacji i pilotażu
Odbiorcy	NGO pomocowe oraz współpracujący z nimi specjaliści, wolontariusze i partnerzy

Sfinansowano ze środków Narodowego Instytutu Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego w ramach Rządowego Programu Fundusz Inicjatyw Obywatelskich NOWEFIO na lata 2021-2030 - Edycja 2026.

Zastrzeżenie: Pakiet jest wzorem organizacyjnym. Nie zastępuje indywidualnej analizy prawnej, obowiązkowych dokumentów ochrony danych, standardów ochrony małoletnich, zasad zgłaszania naruszeń ani wymogów właściwych dla konkretnego zawodu. Organizacja dostosowuje go do swojej działalności i aktualnych przepisów.

Spis treści

Część	Zakres
Wprowadzenie	Podstawa diagnostyczna, problemy z ankiet i zasady korzystania z pakietu.
Część wspólna	Zakres, definicje, role minimalne, trzy poziomy wdrożenia i minimum dokumentacyjne.
Polityka I - Etyka	Godność, kompetencje, granice relacji, konflikt interesów, poufność, wizerunek, AI i naruszenia.
Polityka II - Współpraca	Rekrutacja, wdrożenie, przydział spraw, komunikacja, dokumentacja, zastępstwo, superwizja i zakończenie.
Polityka III - Bezpieczeństwo	Ryzyko, kryzys, praca zdalna i stacjonarna, dane, urządzenia, incydenty, ciągłość i dobrostan.
Wdrożenie	Mapa powiązań z 10 procedurami, scenariusze kontrolne, plan 30 dni i monitoring.
Załączniki	Wzór uchwały, karta konfiguracji, deklaracje, formularz incydentu, checklista i rejestr zmian.

Dokument składa się z części wspólnej, trzech odrębnych polityk oraz załączników wdrożeniowych. Każda polityka może zostać przyjęta i aktualizowana osobno, mimo że cały pakiet jest publikowany w jednym dokumencie.

CZĘŚĆ I | FUNDAMENTY PAKIETU

I

Trzy polityki - jeden spójny system

Najpierw wspólne zasady: proporcjonalność, minimalna dokumentacja, role i trzy poziomy wdrożenia.

01 Diagnoza problemów organizacji pomocowych

02 Wspólne definicje i odpowiedzialność

03 Minimum możliwe do zastosowania także w mikro-NGO

Wprowadzenie

Pakiet powstał jako praktyczna odpowiedź na problemy ujawnione w diagnozie organizacji pomocowych, specjalistów i instytucji współpracujących z NGO. Punktem wyjścia nie jest obraz idealnej, rozbudowanej instytucji, lecz codzienność małych zespołów: ograniczony czas, praca projektowa, wolontariat, kilka ról pełnionych przez jedną osobę, pomoc zdalna i trudne sprawy prowadzone przy niewielkim zapleczu administracyjnym.

Zasada konstrukcyjna: Polityki mają porządkować pracę, a nie produkować dokumentację. Każdy obowiązek powinien chronić beneficjenta, specjalistę lub organizację i mieć możliwie prosty dowód wykonania.

Podstawa diagnostyczna

Wersję 0.9 opracowano na podstawie diagnozy wieloźródłowej obejmującej 120 odpowiedzi badawczych: 65 perspektyw organizacyjnych i instytucjonalnych oraz 55 perspektyw pracowników pomocowych i specjalistów. Materiał pozwala rozpoznać powtarzające się problemy, ale nie stanowi jeszcze ewidencyjnego potwierdzenia udziału 200 unikalnych organizacji. Pakiet pozostaje więc otwarty na korekty wynikające z dalszej walidacji.

Sygnal z diagnozy	Wynik	Odpowiedź w pakiecie
Wysokie lub bardzo wysokie obciążenie administracyjne NGO	16 z 17	Dokumentacja ograniczona do minimum i możliwość łączenia ról.
Potrzeba standardów bezpieczeństwa i dokumentacji	8 z 9 NGO	Jedna polityka bezpieczeństwa i krótkie dowody wdrożenia.
Przeciążenie specjalistów	10 z 19	Prawo zgłoszenia przeciążenia, limity, zastępstwo i superwizja.
Potrzeba wsparcia w deeskalacji i bezpieczeństwie	24 z 36	Ocena ryzyka, eskalacja, przerwanie kontaktu i debriefing.
Brak procedur współpracy instytucji z NGO	20 z 31	Wyznaczony punkt kontaktu, role i zasady przekazania sprawy.

Najważniejsze problemy, które rozwiązują polityki

- Współpraca opiera się na zaangażowaniu konkretnych osób, lecz nie zawsze na trwałych zasadach.
- Role, odpowiedzialność i uprawnienia decyzyjne bywają niejasne.
- Specjalista może rozpocząć pracę bez pełnego wdrożenia do organizacji.
- Dokumentacja spraw i ustaleń jest rozproszona między pocztą, telefonami i prywatnymi komunikatorami.

- Organizacje nie zawsze mają czytelną ścieżkę reagowania na agresję, kryzys psychiczny, zagrożenie życia lub naruszenie poufności.
- Przeciążenie i brak zastępstwa zwiększają ryzyko błędu oraz przerwania pomocy.
- Beneficjent nie zawsze wie, czego może oczekiwać, kto prowadzi jego sprawę i gdzie może zgłosić zastrzeżenia.

Jak korzystać z pakietu

- **Przyjęcie:** Organizacja uzupełnia pola konfiguracyjne, wskazuje osoby odpowiedzialne i przyjmuje pakiet uchwałą, decyzją lub zarządzeniem zgodnym ze swoim sposobem działania.
- **Dostosowanie:** Można skrócić rozwiązania rozszerzone, ale nie należy usuwać minimalnych zasad dotyczących kompetencji, poufności, bezpieczeństwa, eskalacji, dokumentowania, ciągłości pomocy i zgłaszania naruszeń.
- **Powiązanie:** Polityki stanowią poziom nadrzędny. Kroki operacyjne opisują odrębne procedury, a wykonanie potwierdzają wzory dokumentów.
- **Przegląd:** Pakiet przegląda się co najmniej raz w roku oraz po poważnym incydencie, zmianie prawa, zmianie modelu świadczenia pomocy albo powtarzających się skargach.

Część wspólna dla trzech polityk

Cel i zakres

Celem pakietu jest ustanowienie minimalnych, realnych do wdrożenia zasad etycznej, uporządkowanej i bezpiecznej współpracy organizacji pomocowej ze specjalistami. Pakiet chroni trzy strony procesu: osobę korzystającą z pomocy, osobę udzielającą pomocy oraz organizację, która pomoc organizuje i ponosi odpowiedzialność za proces.

- Pakiet stosuje się do członków władz, pracowników, współpracowników, wolontariuszy, praktykantów i stażystów, jeżeli uczestniczą w działaniach pomocowych lub mają dostęp do informacji o beneficjentach.
- Pakiet obejmuje pracę odpłatną i nieodpłatną, stacjonarną, zdalną i hybrydową.
- Zasady stosuje się odpowiednio do współpracy z partnerami, którym przekazywana jest sprawa albo informacja o beneficjencie.
- Jeżeli zasady zawodu regulowanego, umowa, prawo lub wymogi projektu ustanawiają wyższy standard, stosuje się standard wyższy.

Definicje

Pojęcie	Znaczenie w pakiecie
Beneficjent	Osoba korzystająca lub ubiegająca się o pomoc, poradę, interwencję, konsultację albo inne wsparcie.
Specjalista	Osoba wykonująca zadania wymagające wiedzy lub kompetencji szczególnych, m.in. prawnik, psycholog, pedagog, mediator, doradca, interwent, terapeuta, edukator lub superwizor.
Koordynator współpracy	Osoba organizująca pracę specjalistów, przydział spraw, komunikację, dostęp do narzędzi i ciągłość pomocy.
Osoba odpowiedzialna za bezpieczeństwo	Osoba przyjmująca zgłoszenia ryzyka i incydentów oraz uruchamiająca właściwą ścieżkę reakcji.
Sprawa	Wyodrębniony proces pomocy dotyczący beneficjenta albo grupy, posiadający właściciela, cel, minimalną dokumentację i status.
Incydent	Zdarzenie, które spowodowało lub mogło spowodować szkodę, zagrożenie, naruszenie poufności, przerwanie pomocy albo poważne naruszenie zasad.
Eskalacja	Przekazanie decyzji lub ryzyka osobie posiadającej wyższe kompetencje, uprawnienia albo możliwość uruchomienia pomocy zewnętrznej.
Superwizja	Ustrukturyzowane wsparcie merytoryczne i refleksyjne dotyczące pracy pomocowej, prowadzone z zachowaniem poufności i minimalizacji danych.
Kanał zatwierdzony	Narzędzie komunikacji lub przechowywania informacji dopuszczone przez organizację do określonego celu.

Role minimalne

Mała organizacja może łączyć role, jeżeli nie prowadzi to do oceny własnego naruszenia, konfliktu interesów ani braku zastępstwa. Co najmniej jedna osoba pełni rolę koordynatora współpracy, a druga jest wskazana jako zastępca albo zewnętrzny punkt eskalacji.

Rola	Minimalna odpowiedzialność	Czy można łączyć?
Organ zarządzający / osoba kierująca	Przyjęcie polityk, zapewnienie zasobów, decyzje naprawcze.	Tak, z rolą koordynatora w mikro-NGO.
Koordynator współpracy	Wdrożenie specjalistów, przydział spraw, komunikacja, ciągłość.	Tak, z rolą bezpieczeństwa, jeśli istnieje zastępca.
Osoba ds. bezpieczeństwa	Przyjęcie zgłoszenia, ocena pilności, uruchomienie reakcji.	Nie rozpatruje zdarzenia, którego sama dotyczy.
Osoba ds. danych / IOD	Doradztwo w sprawach danych, dostępów i naruszeń.	Może być zewnętrzna.
Superwizor / konsultant	Wsparcie trudnych przypadków i dobrostanu.	Może być zewnętrzny i współdzielony przez kilka NGO.
Specjalista	Praca w granicach kompetencji, dokumentowanie, zgłaszanie ryzyka.	Nie powinien sam zatwierdzać własnego odstępstwa od zasad.

Trzy poziomy wdrożenia

Poziomy mają charakter funkcjonalny, a nie prawny. Organizacja wybiera poziom odpowiadający liczbie spraw, ryzyku i zdolności organizacyjnej. Każda organizacja realizuje minimum; rozwiązania rozszerzone zwiększają jakość, ale nie mogą blokować rozpoczęcia wdrożenia.

Poziom	Dla kogo	Sposób realizacji
MINIMUM	Mikro-NGO, kilka osób, mało spraw.	Jedna karta roli, koordynator i zastępca, zatwierdzone kanały, krótki rejestr spraw i incydentów, dostęp do konsultacji zewnętrznej.
ROZWINIĘTY	Stały zespół i regularne dyżury.	Rozdzielone role, harmonogram superwizji, kwartalny przegląd obciążenia, audyt próbki dokumentacji.
SYSTEMOWY	Wiele zespołów, lokalizacji lub typów usług.	Rejestry centralne, cykliczne szkolenia, analiza trendów, testy scenariuszy, raportowanie do władz organizacji.

Zasada minimalnej dokumentacji

Minimum dowodowe: Dla każdej aktywnej współpracy organizacja powinna móc wskazać: kto działa, na jakiej podstawie, jakie ma zadanie, kto koordynuje, gdzie zapisuje wykonane czynności, jak zgłasza ryzyko oraz kto przejmuje sprawy w razie niedostępności.

- Nie zbiera się danych „na wszelki wypadek”.
- Nie tworzy się kilku formularzy, jeżeli jeden krótki dokument może potwierdzić wykonanie czynności.

- Brak wpisu nie może być automatycznie uzupełniany fikcyjną lub domyślną treścią.
- Dokumentacja ma umożliwić ciągłość pomocy i kontrolę decyzji, a nie odtwarzać każdą rozmowę słowo w słowo.

CZĘŚĆ II | ETYKA

II

Godność, granice i odpowiedzialność

Polityka Etyki porządkuje relację z beneficjentem, granice roli specjalisty, konflikt interesów, poufność i użycie AI.

01 Dobro i podmiotowość osoby korzystającej z pomocy

02 Kompetencje, granice relacji i konflikt interesów

03 Poufność, komunikacja publiczna i narzędzia cyfrowe

POLITYKA I. Etyka i standardy profesjonalnego postępowania

Cel polityki: Zapewnienie, aby pomoc była udzielana z poszanowaniem godności, autonomii, bezpieczeństwa i praw beneficjenta, a osoby działające w imieniu NGO znały granice swojej roli i potrafiły zgłaszać wątpliwości etyczne.

Zasady nadrzędne

- **Dobro i bezpieczeństwo osoby:** Decyzje organizacyjne nie mogą podporządkowywać dobra beneficjenta interesowi wizerunkowemu, statystycznemu ani projektowemu organizacji.
- **Godność i podmiotowość:** Beneficjent nie jest „przypadkiem”, materiałem promocyjnym ani biernym odbiorcą. Ma prawo do informacji, wyboru i odmowy.
- **Nie szkodzić:** Jeżeli działanie może zwiększyć zagrożenie, konflikt, zależność lub ujawnienie danych, należy je zatrzymać, skonsultować lub zmienić.
- **Równe traktowanie:** Pomoc nie może być uzależniana od poglądów, pochodzenia, płci, wieku, niepełnosprawności, sytuacji rodzinnej, orientacji, wyznania ani innych cech niezwiązanych z kryteriami usługi.
- **Rzetelność:** Nie przedstawia się możliwości organizacji, specjalisty ani rezultatu pomocy w sposób przesadzony lub wprowadzający w błąd.
- **Odpowiedzialność:** Każda osoba odpowiada za działania w granicach swojej roli, a organizacja odpowiada za warunki, w których pomoc jest świadczona.

Informowanie i świadomy udział beneficjenta

- Przed rozpoczęciem właściwego wsparcia beneficjent otrzymuje zrozumiałą informację o rodzaju pomocy, osobie prowadzącej, zasadach kontaktu, poufności, dokumentowaniu i możliwości zakończenia kontaktu.
- Nie obiecuje się wyniku, którego specjalista lub organizacja nie może zagwarantować.
- Ograniczenia bezpłatności, liczby kontaktów, terminów lub zakresu działania przekazuje się możliwie wcześnie.
- Zgoda nie może być wymuszana przez presję, ocenianie ani groźbę utraty innego świadczenia, chyba że warunek wynika z prawa lub zasad programu i został jasno wyjaśniony.
- Informację dostosowuje się do wieku, stanu, możliwości komunikacyjnych i potrzeb dostępności beneficjenta.

Kompetencje i granice odpowiedzialności

- Specjalista podejmuje wyłącznie zadania zgodne ze swoim przygotowaniem, doświadczeniem i aktualną zdolnością do bezpiecznej pracy.
- Brak kompetencji, konflikt interesów, przeciążenie, brak warunków technicznych lub brak możliwości zachowania poufności stanowią uzasadnioną podstawę odmowy albo przekazania sprawy.
- Osoba ucząca się, praktykant lub wolontariusz bez samodzielnych kwalifikacji pracuje pod wskazanym nadzorem i nie jest przedstawiana jako samodzielny specjalista.
- Wątpliwość co do diagnozy, interpretacji prawa, ryzyka albo właściwego działania wymaga konsultacji, a nie zgadywania.
- Organizacja nie wywiera presji na specjalistę, aby przekroczył kompetencje tylko dlatego, że brakuje innej osoby.

Praktyczna reguła: Jeżeli osoba nie wie, czy może podjąć decyzję samodzielnie, traktuje to jako sygnał do konsultacji. Brak szybkiej konsultacji nie uprawnia do działania poza kompetencjami, chyba że chodzi o niezwłoczne zabezpieczenie życia lub zdrowia.

Granice relacji

- Kontakt z beneficjentem odbywa się w celu i w ramach uzgodnionej pomocy.
- Nie wykorzystuje się zależności beneficjenta do uzyskania korzyści osobistej, finansowej, emocjonalnej, seksualnej, politycznej lub wizerunkowej.
- Relacje prywatne, intymne lub biznesowe z aktualnym beneficjentem są niedopuszczalne, jeżeli tworzą zależność, konflikt interesów lub ryzyko nadużycia.
- Prezenty o istotnej wartości, pożyczki, przechowywanie pieniędzy oraz prywatne rozliczenia z beneficjentem są niedopuszczalne poza formalnie zatwierdzonym mechanizmem organizacji.
- Kontakt przez prywatne konto lub numer telefonu jest ograniczany. Jeżeli został użyty awaryjnie, istotne ustalenia przenosi się do zatwierdzonego systemu, a dalszy kontakt kieruje do kanału organizacji.
- Specjalista nie staje się jedynym źródłem wsparcia osoby, jeżeli sytuacja wymaga szerszej sieci pomocy.

Konflikt interesów

- Przed przyjęciem sprawy specjalista rozważa, czy zna beneficjenta prywatnie, pozostaje z nim w sporze, zależności albo relacji, która może podważyć bezstronność.
- Konflikt rzeczywisty lub możliwy zgłasza się koordynatorowi przed rozpoczęciem działania albo niezwłocznie po jego ujawnieniu.

- Samo zgłoszenie konfliktu nie jest naruszeniem. Naruszeniem może być jego zatajenie i dalsze samodzielne prowadzenie sprawy.
- Decyzję o wyłączeniu, ograniczeniu zakresu lub dodatkowym nadzorze dokumentuje się krótko, bez ujawniania zbędnych danych osobistych.

Poufność etyczna

- Informacje o beneficjencie omawia się wyłącznie z osobami, które muszą je znać, aby zrealizować pomoc, zapewnić bezpieczeństwo, nadzór lub obowiązki prawne.
- W supervizji i konsultacji wykorzystuje się dane zanonimizowane lub ograniczone do minimum.
- Wyjątek od poufności może wynikać z prawa albo bezpośredniej potrzeby ochrony życia lub zdrowia. Ujawnia się wtedy tylko informacje niezbędne do celu reakcji.
- Jeżeli jest to bezpieczne i możliwe, beneficjent jest informowany o konieczności przekazania informacji oraz o zakresie przekazania.
- Nie omawia się spraw beneficjentów w miejscach publicznych, prywatnych grupach komunikatorów ani w celach towarzyskich.

Wizerunek, historie i komunikacja publiczna

- Historia beneficjenta nie może być publikowana dlatego, że zwiększa szansę promocji lub finansowania.
- Zgoda na wykorzystanie wizerunku lub historii musi być odrębna od zgody na pomoc, dobrowolna i możliwa do wycofania w uzgodnionym zakresie.
- Anonimizacja uwzględnia możliwość rozpoznania osoby po połączeniu kilku szczegółów, nie tylko po nazwisku.
- Nie używa się języka uprzedmiotawiającego, stygmatyzującego ani przedstawiającego NGO jako „wybawcy”.
- W materiałach edukacyjnych i promocyjnych można tworzyć przypadki złożone lub syntetyczne, o ile nie sugeruje się, że są dosłowną historią konkretnej osoby.

Etyka narzędzi cyfrowych i AI

- Narzędzie AI nie zastępuje osądu specjalisty, weryfikacji faktów ani decyzji o bezpieczeństwie.
- Do publicznie dostępnego lub niezatwierdzonego narzędzia nie wprowadza się danych pozwalających zidentyfikować beneficjenta.
- Treści wygenerowane automatycznie podlegają ocenie osoby kompetentnej przed wykorzystaniem wobec beneficjenta.
- Nie przypisuje się AI autorstwa diagnozy, porady prawnej, rekomendacji klinicznej ani decyzji, których system nie może odpowiedzialnie podjąć.

- Jeżeli AI ma istotny wpływ na treść przekazaną beneficjentowi, organizacja określa zasady jego użycia i odpowiedzialność człowieka za wynik.

Zgłaszanie wątpliwości i naruszeń etycznych

- Każda osoba może zgłosić wątpliwość, naruszenie lub presję na działanie nieetyczne bez obowiązku samodzielnego udowodnienia winy.
- Organizacja zapewnia co najmniej jeden poufny kanał zgłoszenia i wskazuje zastępczy kanał, gdy zgłoszenie dotyczy osoby przyjmującej.
- Zgłoszenie rozpatruje osoba bezstronna. Osoba, której dotyczy zgłoszenie, ma prawo przedstawić wyjaśnienia, o ile nie zagraża to bezpieczeństwu ani zabezpieczeniu dowodów.
- Zakazane są działania odwetowe wobec osoby zgłaszającej w dobrej wierze.
- Reakcja może obejmować konsultację, zmianę prowadzącego, ograniczenie dostępu, dodatkowe szkolenie, plan naprawczy, zawieszenie współpracy lub jej zakończenie.
- Celem analizy jest także poprawa systemu, nie tylko ocena jednostki.

Minimalne dowody wdrożenia Polityki Etyki

Wymaganie	Prosty dowód
Zapoznanie z zasadami	Podpisana deklaracja albo elektroniczne potwierdzenie.
Konflikt interesów	Oświadczenie przy rozpoczęciu współpracy i zgłoszenie przy konkretnej sprawie.
Kanał zgłoszeń	Wskazany adres, formularz lub osoba oraz kanał zastępczy.
Reakcja	Krótką kartą zgłoszenia, decyzji i działań naprawczych.
Przegląd	Data rocznego przeglądu i lista wprowadzonych zmian.

CZĘŚĆ III | WSPÓŁPRACA

III

Jasne role, bezpieczne przekazanie i ciągłość

Polityka Współpracy prowadzi organizację przez cały cykl: od rekrutacji i wdrożenia specjalisty po zakończenie współpracy.

01 Właściciel procesu i jednoznaczna odpowiedzialność

02 Przydział spraw, dokumentowanie i zastępstwo

03 Superwizja, prawo odmowy i bezpieczny offboarding

POLITYKA II. Współpraca NGO ze specjalistami

Cel polityki: Zapewnienie ciągłego i przewidywalnego cyklu współpracy: od wyboru i wdrożenia specjalisty, przez przydział oraz dokumentowanie spraw, po zastępstwo, ocenę jakości i bezpieczne zakończenie współpracy.

Zasada właściciela procesu

Każda aktywna współpraca i każda sprawa posiada osobę odpowiedzialną za koordynację. Odpowiedzialność specjalisty za treść własnych działań nie zwalnia organizacji z odpowiedzialności za sposób zorganizowania pracy, dostęp do narzędzi, komunikację i reakcję na ryzyko.

- Koordynator i jego zastępca są znani specjalistom.
- Beneficjent wie, kto prowadzi jego sprawę lub gdzie uzyska informację organizacyjną.
- Nie przydziela się sprawy wyłącznie przez nieudokumentowaną wiadomość prywatną.
- Zmiana osoby prowadzącej wymaga przekazania minimum informacji niezbędnych do ciągłości.

Formy współpracy

- Współpraca może opierać się na zatrudnieniu, umowie cywilnoprawnej, działalności gospodarczej, wolontariacie, praktyce, stażu lub porozumieniu partnerskim.
- Forma prawna nie może służyć do ukrywania rzeczywistej odpowiedzialności, pomijania zasad poufności ani dopuszczania do pracy bez wdrożenia.
- Wolontariusz specjalistyczny podlega tym samym standardom merytorycznym i bezpieczeństwa co osoba odpłatna wykonująca to samo zadanie.
- Praktykant albo osoba przygotowująca się do zawodu ma jasno określony zakres i nadzór.

Rekrutacja i weryfikacja

- Organizacja opisuje rzeczywiste zadania i wymagania, nie zawyżając ani nie zaniżając roli.
- Zakres weryfikacji jest proporcjonalny do ryzyka. Może obejmować wykształcenie, doświadczenie, uprawnienia, referencje, prawo wykonywania zawodu, ubezpieczenie albo inne wymagania właściwe dla roli.
- Weryfikacja kwalifikacji jest odnotowana w checkliście; nie ma potrzeby kopiowania wszystkich dokumentów, jeżeli wystarczy potwierdzenie sprawdzenia.
- Przed dopuszczeniem do danych i kontaktu z beneficjentem ustala się konflikt interesów, zakres samodzielności i osobę nadzorującą.

- Braki możliwe do uzupełnienia prowadzą do planu wdrożenia, a nie do fikcyjnego potwierdzenia spełnienia wymagań.

Minimalna treść ustaleń ze specjalistą

Element	Co musi być jasne
Rola	Jakie działania specjalista wykonuje, a jakich nie wykonuje.
Odpowiedzialność	Kto podejmuje decyzje merytoryczne, organizacyjne i kryzysowe.
Dostępność	Dyżury, termin odpowiedzi, sposób zgłoszenia nieobecności.
Dokumentacja	Co zapisuje, gdzie, w jakim terminie i kto ma dostęp.
Komunikacja	Zatwierdzone kanały i osoby kontaktowe.
Poufność i dane	Zakres dostępu, minimalizacja, retencja, zwrot lub usunięcie materiałów.
Superwizja	Czy i jak specjalista korzysta z konsultacji lub superwizji.
Zastępstwo	Kto przejmuje sprawy w razie nieobecności.
Zakończenie	Sposób przekazania spraw, odebrania dostępów i poinformowania beneficjentów.

Wdrożenie specjalisty

Dopuszczenie do samodzielnego kontaktu z beneficjentem następuje po przekazaniu minimum organizacyjnego.

- cel i zakres działalności organizacji;
- karta roli oraz granice odpowiedzialności;
- koordynator, zastępca i ścieżka eskalacji;
- zasady etyczne, poufność i konflikt interesów;
- minimalna dokumentacja i miejsce jej prowadzenia;
- zatwierdzone kanały kontaktu oraz zasady pracy zdalnej;
- procedura bezpieczeństwa, interwencji kryzysowej i incydentu;
- zasady superwizji, konsultacji oraz zgłaszania przeciążenia;
- zasady skarg, informacji zwrotnej i zakończenia współpracy.

Mikro-NGO: Wdrożenie może odbyć się podczas jednego spotkania i zostać potwierdzone jedną checklistą. Nie ma potrzeby tworzenia osobnego szkolenia do każdego punktu.

Przyjmowanie i przydzielanie spraw

- Każde zgłoszenie otrzymuje minimalny status: nowe, zakwalifikowane, przydzielone, w toku, oczekujące, przekazane albo zakończone.
- Przed przydzieleniem ocenia się co najmniej rodzaj potrzeby, pilność, ryzyko, właściwość organizacji, wymagane kompetencje i dostępność.
- Specjalista potwierdza przyjęcie sprawy. Brak odpowiedzi nie jest równoznaczny z przyjęciem.

- Sprawa wysokiego ryzyka nie jest przekazywana osobie bez odpowiedniego przygotowania lub dostępu do konsultacji.
- Jeżeli organizacja nie może udzielić pomocy, informuje o tym możliwie szybko i - w granicach możliwości - wskazuje bezpieczny kierunek dalszego kontaktu.

Prawo odmowy i zgłoszenie przeciążenia

- Specjalista może odmówić przyjęcia albo dalszego prowadzenia sprawy z powodu braku kompetencji, konfliktu interesów, przeciążenia, ryzyka osobistego, braku warunków poufności lub innej uzasadnionej przeszkody.
- Odmowa jest zgłaszana koordynatorowi i krótko uzasadniona; nie wymaga ujawniania prywatnych informacji zdrowotnych ponad niezbędny zakres.
- Zgłoszenie przeciążenia nie może automatycznie prowadzić do sankcji lub negatywnej oceny.
- Koordynator podejmuje decyzję o ograniczeniu liczby spraw, zmianie priorytetów, zastępstwie, konsultacji albo przerwie.
- Sprawa nie może zostać porzucona. Jeżeli specjalista musi natychmiast przerwać pracę, organizacja uruchamia plan ciągłości.

Komunikacja i ustalenia

- Organizacja wskazuje, które kanały służą do spraw organizacyjnych, a które do kontaktu z beneficjentem.
- Decyzje dotyczące przydziału, ryzyka, zmiany zakresu, przekazania lub zakończenia sprawy zapisuje się w systemie albo krótkiej karcie.
- Pilne wiadomości mają określony sposób oznaczenia i kanał. Wiadomość w zwykłym komunikatorze nie może być jedynym mechanizmem alarmowym.
- Ustala się realny czas odpowiedzi. Organizacja nie deklaruje całodobowej dostępności, jeżeli jej faktycznie nie zapewnia.
- W komunikacji zespołowej przekazuje się tylko informacje niezbędne danej osobie.

Dokumentowanie pracy

Minimalna notatka powinna pozwolić innej uprawnionej osobie zrozumieć, co zostało zrobione i jaka jest kolejna bezpieczna czynność. Nie wymaga stenogramu ani opisu życia beneficjenta ponad cel pomocy.

- data i forma kontaktu;
- cel lub temat kontaktu;
- najważniejsze ustalenie, udzielona informacja lub działanie;
- rozpoznane ryzyko i podjęta reakcja, jeśli wystąpiły;
- uzgodniony kolejny krok, termin albo sposób zakończenia oraz autor wpisu.

Współpraca interdyscyplinarna i przekazanie sprawy

- Konsultację uruchamia się, gdy sprawa przekracza kompetencje jednej osoby, zawiera sprzeczne potrzeby albo wysokie ryzyko.
- Przed konsultacją ustala się jej cel i ogranicza dane do niezbędnych.
- Po konsultacji dokumentuje się wniosek i osobę odpowiedzialną za kolejną czynność, nie pełny przebieg dyskusji.
- Przekazanie sprawy wymaga potwierdzenia przyjęcia przez nową osobę. Samo wysłanie wiadomości nie kończy odpowiedzialności przekazującego.
- Beneficjent jest informowany o zmianie osoby, jeżeli nie zwiększa to ryzyka i jest możliwe.

Współpraca zdalna i hybrydowa

- Przed rozpoczęciem kontaktu ustala się, czy forma zdalna jest odpowiednia do potrzeby i ryzyka.
- Specjalista korzysta z zatwierdzonego konta i chroni prywatne dane kontaktowe.
- W sprawach o podwyższonym ryzyku ustala się sposób działania na wypadek przerwania połączenia.
- Istotne ustalenia z wideorozmowy, czatu lub telefonu trafiają do dokumentacji sprawy.
- Nagrywanie nie jest domyślne i wymaga odrębnej podstawy, celu, informacji oraz bezpiecznego przechowywania.

Jakość, informacja zwrotna i skargi

- Jakość ocenia się na podstawie organizacji pracy, terminowości, zgodności z rolą, dokumentacji, bezpieczeństwa i doświadczenia beneficjenta - nie tylko liczby obsłużonych osób.
- Organizacja zapewnia prosty sposób przekazania uwagi lub skargi.
- Skarga dotycząca specjalisty nie jest automatycznie rozpatrywana przez tę samą osobę.
- Powtarzające się problemy prowadzą do zmiany systemu, instrukcji, szkolenia albo obciążenia, nawet jeśli nie doszło do poważnego incydentu.
- Ocena jakości nie może wymuszać na beneficjencie ujawniania dodatkowych danych.

Superwizja i konsultacja

- Organizacja zapewnia dostęp do superwizji, konsultacji przypadku albo innej adekwatnej formy wsparcia, proporcjonalnie do ryzyka pracy.
- Superwizja jest elementem organizacji pracy, a nie wyłącznie aktywnością po godzinach.
- W superwizji nie ujawnia się danych ponad niezbędny zakres.
- Po zdarzeniu krytycznym zapewnia się możliwość szybkiego debriefingu i decyzji o dalszym obciążeniu.

- Brak stałego supervizora wewnętrznego może być zastąpiony współpracą z osobą zewnętrzną albo grupą międzyorganizacyjną.

Zakończenie współpracy i offboarding

- Przed zakończeniem współpracy sporządza się listę aktywnych spraw i status ich przekazania.
- Specjalista uzupełnia minimalną dokumentację, zwraca powierzony sprzęt i materiały oraz przekazuje informacje niezbędne do ciągłości.
- Organizacja odbiera lub zamyka dostęp nie później niż w terminie wynikającym z ryzyka, co do zasady w dniu zakończenia aktywności.
- Beneficjenci wymagający dalszej pomocy otrzymują informację o zmianie i nowym kanale kontaktu.
- Zakończenie współpracy nie znosi obowiązku poufności.

Minimalne dowody wdrożenia Polityki Współpracy

Etap	Dowód minimalny
Dopuszczenie	Karta roli i checklista kwalifikacji.
Wdrożenie	Podpisana checklista obejmująca etykę, bezpieczeństwo, dane i dokumentację.
Przydział	Status sprawy, osoba prowadząca i potwierdzenie przyjęcia.
Prowadzenie	Minimalna notatka oraz zapis decyzji i ryzyka.
Zastępstwo	Wskazana osoba przejmująca i karta przekazania.
Zakończenie	Lista spraw, odebranie dostępów i potwierdzenie zwrotu materiałów.

CZĘŚĆ IV | BEZPIECZEŃSTWO

IV

Ochrona ludzi, informacji i ciągłości pomocy

Bezpieczeństwo obejmuje nie tylko kryzys, lecz także codzienną pracę zdalną, dane, urządzenia, dobrostan i zdolność organizacji do działania.

01 Ocena ryzyka i poziomy reakcji

02 Bezpieczny kontakt zdalny i stacjonarny

03 Dane, incydenty, ciągłość działania i dobrostan kadry

POLITYKA III. Bezpieczeństwo beneficjentów, kadry, informacji i procesów

Cel polityki: Zapobieganie możliwej do uniknięcia szkodzi oraz zapewnienie, że organizacja rozpoznaje ryzyko, reaguje proporcjonalnie, dokumentuje incydenty i wspiera osoby uczestniczące w trudnych zdarzeniach.

Zakres bezpieczeństwa

- **Beneficjent:** ochrona życia, zdrowia, godności, prywatności i ciągłości pomocy.
- **Specjalista:** ochrona przed agresją, nękaniami, ekspozycją danych, przeciążeniem i pozostawieniem bez wsparcia.
- **Informacja:** poufność, integralność, dostępność i ograniczony dostęp.
- **Proces:** czytelne role, zastępstwo, eskalacja, dokumentowanie i ciągłość działania.
- **Organizacja:** ograniczenie ryzyka prawnego, operacyjnego i wizerunkowego przez rzeczywiste działanie, nie sam dokument.

Ocena ryzyka sprawy

Ocena ryzyka jest krótka i proporcjonalna. Nie zastępuje diagnozy medycznej ani profesjonalnej oceny właściwej dla zawodu. Służy decyzji organizacyjnej: kto powinien działać, jak pilnie, w jakiej formie i z jakim wsparciem.

- Czy występuje bezpośrednio lub szybko narastające zagrożenie życia albo zdrowia?
- Czy osoba mówi o samouszkodzeniu, samobójstwie, przemocy lub skrzywdzeniu innej osoby?
- Czy zagrożone jest dziecko, osoba zależna albo osoba o ograniczonej możliwości ochrony siebie?
- Czy występuje agresja, groźby, stalking, przemoc domowa, przemoc seksualna lub inne wysokie ryzyko?
- Czy specjalista posiada kompetencje i warunki do bezpiecznego działania?
- Czy kontakt zdalny jest wystarczający, a w razie przerwania istnieje plan dalszej reakcji?
- Czy sprawa wymaga natychmiastowej eskalacji, konsultacji, przekazania lub uruchomienia właściwych służb?

Poziomy reakcji

Poziom	Przykładowa sytuacja	Minimalna reakcja
ZIELONY	Brak rozpoznanych sygnałów podwyższonego ryzyka.	Zwykły tok pomocy, dokumentacja, monitorowanie zmiany.
ŻÓŁTY	Niepewność, narastające emocje, niepełne dane, ryzyko przekroczenia kompetencji.	Konsultacja, plan bezpieczeństwa, częstszy kontakt lub zmiana osoby/formy.
CZERWONY	Bezpośrednie zagrożenie życia, zdrowia, poważna przemoc albo zdarzenie wymagające pilnej reakcji.	Niezwłoczna eskalacja, zabezpieczenie osoby i uruchomienie właściwych służb lub procedur.

Ważne: Polityka nie wymaga od wolontariusza ani koordynatora podejmowania decyzji klinicznych lub prawnych poza kompetencjami. Wymaga natomiast rozpoznania alarmu, przerwania zwykłego trybu i wezwania właściwego wsparcia.

Reagowanie na zagrożenie życia lub zdrowia

- Osoba prowadząca nie pozostaje sama z decyzją wysokiego ryzyka, o ile kontakt z koordynatorem lub służbami jest możliwy.
- Najpierw zabezpiecza się życie i zdrowie, następnie dokumentację oraz analizę formalną.
- Wzywa się właściwe służby ratunkowe lub interwencyjne, gdy sytuacja tego wymaga; organizacja utrzymuje aktualną lokalną listę kontaktów.
- Zakres przekazywanych informacji ogranicza się do tego, co niezbędne do reakcji.
- Po ustaniu bezpośredniego zagrożenia sporządza się kartę incydentu, zabezpiecza ciągłość pomocy i organizuje debriefing.
- Jeżeli procedura nie zadziałała, organizacja analizuje przyczynę systemową i wprowadza działanie naprawcze.

Bezpieczeństwo kontaktu zdalnego

- Na początku współpracy beneficjent otrzymuje informację, do czego służy kanał zdalny, w jakich godzinach działa i co zrobić poza nimi.
- W sprawie o podwyższonym ryzyku ustala się minimalne dane umożliwiające reakcję w razie utraty kontaktu, o ile jest to adekwatne i zgodne z zasadami danych.
- Jeżeli połączenie zostaje przerwane w momencie rozpoznanego zagrożenia, specjalista wykonuje uzgodniony plan: ponawia kontakt, informuje koordynatora i podejmuje dalsze kroki proporcjonalne do ryzyka.
- Specjalista nie prowadzi rozmowy wymagającej poufności w miejscu, w którym osoby postronne mogą ją usłyszeć.
- Nie używa się prywatnych kont społecznościowych jako podstawowego kanału poradnictwa.

- Kontakt zdalny jest przenoszony do formy stacjonarnej lub innej instytucji, jeżeli zdalność nie zapewnia bezpieczeństwa lub jakości.

Bezpieczeństwo spotkań stacjonarnych

- Miejsce kontaktu zapewnia możliwie bezpieczne wyjście, prywatność i możliwość wezwania wsparcia.
- Osoba nieprzeszkolona nie prowadzi sama spotkania uznanego za wysokiego ryzyka.
- Przy przewidywanym ryzyku agresji ustala się obecność drugiej osoby, sposób przerywania spotkania i kanał alarmowy.
- Specjalista ma prawo przerwać spotkanie przy groźbach, przemocy, naruszeniu granic lub braku warunków bezpiecznej pracy.
- Przerwanie spotkania nie oznacza porzucenia sprawy: koordynator ocenia dalszy bezpieczny sposób kontaktu lub przekazania.

Agresja, groźby, stalking i nękanie

- Groźby i nękanie nie są traktowane jako „normalny koszt pomagania”.
- Specjalista nie negocjuje samodzielnie z osobą, która kieruje poważne groźby wobec niego, jego rodziny lub organizacji.
- Zabezpiecza się dowody w sposób zgodny z prawem i ogranicza dalszą ekspozycję danych kontaktowych.
- Organizacja może zmienić kanał kontaktu, wyznaczyć drugą osobę, ograniczyć bezpośredni kontakt albo uruchomić pomoc instytucjonalną.
- Po zdarzeniu ocenia się potrzebę wsparcia psychologicznego, prawnego, organizacyjnego i przerwy w pracy.

Dzieci i osoby szczególnie narażone

- W pracy z dzieckiem lub osobą zależną stosuje się dodatkowe zasady ochrony właściwe dla działalności organizacji.
- Pakiet nie zastępuje odrębnych standardów ochrony małoletnich, jeżeli organizacja ma obowiązek lub potrzebę ich stosowania.
- Informację przekazuje się w sposób zrozumiały, a obecność opiekuna ocenia się z uwzględnieniem bezpieczeństwa i możliwego konfliktu interesów.
- Podejrzanie krzywdzenia jest eskalowane zgodnie z właściwą procedurą, nie pozostawiane do prywatnej decyzji niedoświadczonej osoby.
- Nie ujawnia się opiekunowi informacji, jeżeli mogłoby to zwiększyć zagrożenie i sprzeciwia się właściwym zasadom ochrony.

Dane, poufność i minimalizacja

- Organizacja określa cel, zakres i miejsce prowadzenia dokumentacji oraz osoby uprawnione do dostępu.
- Dane szczególnie wrażliwe lub opisujące kryzys nie są gromadzone tylko dlatego, że mogą „kiedyś się przydać”.
- Dostęp przyznaje się według roli i odbiera niezwłocznie po ustaniu potrzeby.
- Dokumentów beneficjentów nie przechowuje się w prywatnej poczcie, galerii telefonu ani niezatwierdzonym komunikatorze.
- Wydruków i notatek roboczych nie pozostawia się w miejscu dostępnym dla osób postronnych.
- Okres przechowywania i sposób bezpiecznego usunięcia określa organizacja z uwzględnieniem celu, prawa, umów i ochrony roszczeń.

Urządzenia, konta i kanały komunikacji

- Każda osoba korzysta z indywidualnego konta; nie udostępnia hasła innym członkom zespołu.
- Tam, gdzie to możliwe, organizacja stosuje uwierzytelnianie wieloskładnikowe.
- Urządzenie używane do pracy jest zabezpieczone blokadą, aktualizowane i chronione przed dostępem osób postronnych.
- Organizacja prowadzi listę zatwierdzonych narzędzi oraz sposób zgłaszania awarii, phishingu lub utraty urządzenia.
- Jeżeli prywatne urządzenie jest dopuszczone, organizacja określa minimalne warunki użycia i usunięcia danych po zakończeniu współpracy.
- Kopie bezpieczeństwa i możliwość odzyskania kluczowej dokumentacji są testowane proporcjonalnie do skali działania.

Bezpieczeństwo korzystania z AI

- Do narzędzi AI nie wprowadza się danych identyfikujących beneficjenta ani pełnych opisów spraw, chyba że organizacja dopuściła konkretne narzędzie po analizie i istnieje odpowiednia podstawa oraz zabezpieczenia.
- AI nie podejmuje samodzielnie decyzji o pilności, ryzyku, odmowie pomocy, diagnozie ani przekazaniu danych.
- Treść przygotowana z pomocą AI jest weryfikowana pod względem faktów, kompetencji, języka i możliwej szkody.
- W przypadku błędu odpowiedzialność za przekazaną treść ponosi osoba i organizacja, które ją zatwierdziły, a nie narzędzie.

Incydenty i naruszenia

- Incydent zgłasza się niezwłocznie przez wskazany kanał, nawet jeśli nie jest jeszcze znany pełny skutek.
- Pierwsza reakcja obejmuje ograniczenie szkody, zabezpieczenie osoby i informacji oraz powiadomienie właściwego właściciela procesu.
- Zgłaszający opisuje fakty, nie przypuszczając winę.
- Organizacja określa, czy zdarzenie wymaga dalszych obowiązków prawnych, zawiadomienia partnera, osoby, służb albo organu.
- Każdy incydent otrzymuje właściciela, termin działania i status zamknięcia.
- Analiza przyczyn obejmuje warunki pracy, obciążenie, brak szkolenia, narzędzia, komunikację i procedury.

Ciągłość działania

- Organizacja wskazuje zastępstwo dla kluczowych ról i sposób przejęcia aktywnych spraw.
- Istnieje plan działania na wypadek niedostępności systemu, poczty, telefonu, koordynatora albo lokalu.
- Lista spraw nie może istnieć wyłącznie w pamięci jednej osoby.
- W razie awarii dokumentuje się minimum w bezpieczny sposób zastępczy, a następnie przenosi do systemu bez tworzenia duplikatów.
- Priorytet mają sprawy o wysokim ryzyku i osoby, dla których przerwanie kontaktu może spowodować szkodę.

Dobrostan i bezpieczeństwo psychiczne kadry

- Organizacja monitoruje nie tylko liczbę spraw, ale również ich ciężar emocjonalny, pilność i kumulację zdarzeń trudnych.
- Specjalista może zgłosić przeciążenie, potrzebę konsultacji albo czasowego wyłączenia z określonego rodzaju spraw.
- Po incydencie krytycznym koordynator kontaktuje się z osobą prowadzącą, organizuje debriefing i ocenia zdolność do dalszej pracy.
- Superwizja nie służy kontroli dyscyplinarnej ani publicznemu ocenianiu osoby.
- Wolontariusz lub praktykant nie może pozostawać jedyną osobą odpowiedzialną za sprawę wysokiego ryzyka.
- Jeżeli organizacja nie ma zasobów wewnętrznych, zapewnia dostęp do konsultacji zewnętrznej lub współdzielonej.

Minimalne dowody wdrożenia Polityki Bezpieczeństwa

Wymaganie	Dowód minimalny
Role i kontakty	Koordinator, zastępca, osoba ds. bezpieczeństwa i lista kontaktów zewnętrznych.
Ocena ryzyka	Krótką karta lub pole w systemie dla spraw wymagających oceny.
Kanały i dostępy	Lista zatwierdzonych narzędzi i rejestr dostępu.
Incydenty	Karta incydentu z właścicielem, reakcją i statusem.
Ciągłość	Lista zastępstw i sposób dostępu do aktywnych spraw.
Dobrostan	Możliwość zgłoszenia przeciążenia, harmonogram konsultacji lub superwizji.
Przegląd	Analiza po zdarzeniu oraz roczny test zasad.

CZĘŚĆ V | WDROŻENIE I NARZĘDZIA

V

Od uchwały do codziennej praktyki

Ta część łączy polityki z procedurami, scenariuszami kontrolnymi, planem wdrożenia oraz siedmioma gotowymi załącznikami.

01 Mapa powiązań z procedurami Standardów NGO 1.0

02 Plan 30 dni i monitoring bez nadmiaru biurokracji

03 Uchwała, konfiguracja, deklaracje, zgłoszenie i checklisty

PLUS HELP NGO | PAKIET MODELOWYCH POLITYK 0.9

Powiązanie polityk z procedurami Standardów NGO 1.0

Polityki określają zasady i odpowiedzialność. Nie zastępują procedur opisujących kolejne czynności. Poniższa mapa zapobiega dublowaniu treści i pozwala wykazać odrębne rezultaty projektu.

Procedura wykonawcza	Etyka	Współpraca	Bezpieczeństwo
1. Rekrutacja, weryfikacja i dopuszczenie specjalisty	kompetencje, konflikt	wybór, rola, forma	dostęp, ryzyko roli
2. Wdrożenie organizacyjne specjalisty	deklaracja zasad	checklista wdrożenia	kanały, eskalacja
3. Przyjęcie, kwalifikacja i przekazanie sprawy	informacja i zgoda	przydział i potwierdzenie	ocena ryzyka
4. Prowadzenie i dokumentowanie wsparcia	rzetelność, granice	minimum wpisu	poufność i dostęp
5. Bezpieczeństwo beneficjenta i specjalisty	nie szkodzić	role i zastępstwo	reakcja i incydent
6. Interwencja kryzysowa	wyjątek od poufności	koordynacja	eskalacja i służby
7. Dane, poufność i praca online	poufność	zatwierdzone kanały	ochrona informacji
8. Komunikacja i konsultacja interdyscyplinarna	minimalizacja danych	terminy i decyzje	eskalacja ryzyka
9. Superwizja, debriefing i przeciążenie	odpowiedzialność	organizacja pracy	dobrostan po incydencie
10. Skargi, incydenty i zakończenie wsparcia	bezstronność	ciągłość i offboarding	reakcja naprawcza

Sześć sytuacji kontrolnych

Specjalista nie odpowiada i ma aktywne sprawy: Koordynator uruchamia zastępstwo, sprawdza ryzyko, dokumentuje przekazanie i ogranicza dostęp, jeżeli współpraca faktycznie ustała.

Beneficjent pisze na prywatny profil specjalisty: Specjalista przenosi kontakt do kanału organizacji, zapisuje istotne ustalenie i nie rozwija równoległej relacji prywatnej.

W rozmowie online pojawia się zagrożenie życia: Specjalista uruchamia plan przerwanego połączenia i eskalację, przekazuje wyłącznie niezbędne dane, a po zdarzeniu sporządza kartę incydentu i korzysta z debriefingu.

Specjalista jest przeciążony: Zgłasza to bez sankcji. Koordynator zmniejsza obciążenie, ustala priorytety i zapewnia przekazanie spraw wymagających ciągłości.

Organizacja chce opublikować historię sukcesu: Oddziela pomoc od zgody promocyjnej, ocenia możliwość rozpoznania osoby, ogranicza szczegóły i respektuje odmowę bez wpływu na wsparcie.

Nie wiadomo, kto ma podjąć decyzję: Sprawa nie pozostaje w próżni. Osoba prowadząca eskaluje ją do wskazanego koordynatora lub zastępcy i zapisuje decyzję oraz właściciela kolejnego kroku.

Wdrożenie pakietu w organizacji

Pakiet można wdrożyć w ciągu 30 dni bez tworzenia rozbudowanej administracji. Warunkiem jest podjęcie kilku konkretnych decyzji i ich zakomunikowanie zespołowi.

1. Uzupełnić Kartę konfiguracji organizacji.
2. Wyznaczyć koordynatora współpracy, zastępcę, osobę ds. bezpieczeństwa i punkt kontaktu w sprawach danych.
3. Porównać pakiet z istniejącymi regulaminami i usunąć sprzeczności.
4. Ustalić zatwierdzone kanały komunikacji, dokumentacji i przechowywania danych.
5. Przyjąć pakiet właściwą uchwałą, decyzją albo zarządzeniem.
6. Przeprowadzić jedno wspólne szkolenie obejmujące trzy polityki oraz scenariusze kryzysowe.
7. Zebrać potwierdzenia zapoznania się z politykami i oświadczenia wymagane dla ról.
8. Przetestować jedną ścieżkę: przyjęcie sprawy - przydział - dokumentacja - przekazanie - zakończenie.
9. Przetestować scenariusz awarii albo incydentu i poprawić niejasne punkty.
10. Po 30 dniach zebrać krótką informację zwrotną od specjalistów i przyjąć listę zmian.

Monitoring bez nadmiaru biurokracji

Co sprawdzamy	Jak często	Prosty miernik
Wdrożenie specjalistów	przy rozpoczęciu i kwartalnie	odsetek aktywnych osób z kompletną checklistą
Dostęp do procedur bezpieczeństwa	kwartalnie	odsetek aktywnych osób z potwierdzonym dostępem
Kompletność dokumentacji	kwartalnie, na próbce	czy wpis pozwala ustalić działanie, ryzyko i kolejny krok
Przeciążenie	co najmniej kwartalnie	liczba osób zgłaszających wysokie obciążenie i podjęta reakcja
Incydenty	na bieżąco i kwartalnie zbiorczo	czas reakcji, właściciel i zamknięcie działania naprawczego
Ciągłość	kwartalnie	liczba spraw przerwanych bez przekazania

Co sprawdzamy	Jak często	Prosty miernik
Jakość współpracy	półrocznie	krótka ocena NGO, specjalistów i - jeśli możliwe - beneficjentów

Przegląd i aktualizacja

- Pakiet jest przeglądany co najmniej raz w roku.
- Przegląd uruchamia się także po poważnym incydencie, zmianie modelu usług, istotnej zmianie prawa, powtarzających się skargach lub wnioskach z supervizji.
- Zmiany są wersjonowane i opisane w rejestrze zmian.
- Osoby objęte zmianą otrzymują informację i - gdy to potrzebne - krótkie szkolenie.
- Odstępstwo od polityki wymaga uzasadnienia, wskazania osoby zatwierdzającej, czasu obowiązywania i środka ograniczającego ryzyko.

ZAŁĄCZNIK 1. Wzór uchwały lub decyzji o przyjęciu pakietu

UCHWAŁA / DECYZJA NR _____

z dnia _____

w sprawie przyjęcia „Pakietu Modelowych Polityk Organizacyjnych dla NGO Pomocowych: Etyka - Współpraca - Bezpieczeństwo”.

1. Przyjmuje się do stosowania Pakiet Modelowych Polityk Organizacyjnych dla NGO Pomocowych w wersji _____, stanowiący załącznik do niniejszej uchwały / decyzji.
2. Do stosowania pakietu zobowiązane są osoby wykonujące zadania pomocowe, koordynacyjne, administracyjne i zarządcze w zakresie odpowiadającym ich roli.
3. Koordynatorem wdrożenia zostaje _____.
4. Osobą odpowiedzialną za bezpieczeństwo zostaje _____, a zastępcą _____.
5. Osobą lub punktem kontaktu w sprawach ochrony danych zostaje _____.
6. Polityki wchodzi w życie z dniem _____. Przegląd wdrożenia nastąpi do dnia _____.

Podpis osoby / osób uprawnionych: _____

ZAŁĄCZNIK 2. Karta konfiguracji organizacji

Nazwa organizacji:

Wersja pakietu i data przyjęcia:

Koordynator współpracy: _____

Zastępca koordynatora: _____

Osoba ds. bezpieczeństwa: _____

Osoba / punkt kontaktu ds. danych: _____

Superwizor / źródło konsultacji: _____

Obszar	Ustalenie organizacji
Kanał organizacyjny zespołu	
Kanał kontaktu z beneficjentem	
Miejsce dokumentacji spraw	
Kanał pilnej eskalacji	
Kanał zgłoszeń etycznych	
Kanał zgłoszeń incydentów	
Kanał zastępczy	
Godziny dostępności	
Sposób działania poza godzinami	
Sposób zgłoszenia przeciążenia	
Zewnętrzne kontakty kryzysowe	
Termin corocznego przeglądu	

ZAŁĄCZNIK 3. Deklaracja zapoznania się z pakietem

Imię i nazwisko: _____

Rola / funkcja: _____

Oświadczam, że zapoznałam(-em) się z Pakietem Modelowych Polityk Organizacyjnych dla NGO Pomocowych: Etyka - Współpraca - Bezpieczeństwo, rozumiem zasady dotyczące mojej roli i wiem, gdzie znajdują się procedury oraz wzory dokumentów.

- zobowiązuję się działać w granicach kompetencji i powierzonej roli;
- zobowiązuję się chronić informacje poufne i korzystać z zatwierdzonych kanałów;
- wiem, komu zgłosić ryzyko, incydent, konflikt interesów i przeciążenie;
- rozumiem, że poufność obowiązuje także po zakończeniu współpracy;
- zobowiązuję się nie wprowadzać danych beneficjentów do niezatwierdzonych narzędzi, w tym narzędzi AI.

Data i podpis / potwierdzenie elektroniczne:

ZAŁĄCZNIK 4. Oświadczenie o konflikcie interesów

Imię i nazwisko: _____

Rola / sprawa, której dotyczy oświadczenie:

Zaznacz właściwe:

- ☐ Nie jest mi znany konflikt interesów mogący wpływać na wykonywanie powierzonych roli / prowadzenie sprawy.
- ☐ Zgłaszam rzeczywisty lub możliwy konflikt interesów i proszę o decyzję koordynatora.

Krótki opis konfliktu lub ryzyka: _____

Proponowany sposób ograniczenia ryzyka:

Decyzja koordynatora: _____

Data, podpis / potwierdzenie: _____

ZAŁĄCZNIK 5. Karta zgłoszenia etycznego lub incydentu

Data i godzina zdarzenia / ujawnienia: _____

Osoba zgłaszająca i kontakt: _____

Kanał zgłoszenia: _____

Rodzaj zgłoszenia:

- ☐ wątpliwość etyczna
- ☐ konflikt interesów
- ☐ zagrożenie beneficjenta
- ☐ zagrożenie specjalisty
- ☐ naruszenie poufności lub danych
- ☐ agresja, groźby lub nękanie
- ☐ przerwanie ciągłości pomocy
- ☐ inne

Opis faktów - co się wydarzyło: _____

Czy istnieje bieżące zagrożenie i dla kogo: _____

Działanie podjęte natychmiast: _____

Osoby / instytucje powiadomione: _____

Właściciel dalszych działań i termin: _____

Działanie naprawcze: _____

Data i sposób zamknięcia: _____

ZAŁĄCZNIK 6. Checklista minimalnego wdrożenia

Nr	Punkt kontrolny	Tak
1	Pakiet został formalnie przyjęty i posiada numer wersji.	☐
2	Wyznaczono koordynatora współpracy i zastępcę.	☐
3	Wyznaczono osobę odpowiedzialną za bezpieczeństwo.	☐
4	Wskazano punkt kontaktu w sprawach danych.	☐
5	Każdy specjalista ma kartę roli i zweryfikowane kompetencje.	☐
6	Każdy aktywny specjalista przeszedł udokumentowane wdrożenie.	☐
7	Specjaliści podpisali deklarację poufności i zasad etycznych.	☐
8	Istnieje prosty sposób zgłoszenia konfliktu interesów.	☐
9	Każda sprawa ma status, osobę prowadzącą i kolejny krok.	☐
10	Organizacja prowadzi minimalną dokumentację kontaktów.	☐
11	Ustalono zatwierdzone kanały komunikacji i przechowywania.	☐
12	Ustalono sposób pilnej eskalacji i działania przy utracie kontaktu.	☐
13	Istnieje kanał zgłaszania incydentów i naruszeń.	☐
14	Istnieje zastępstwo dla aktywnych spraw.	☐
15	Specjaliści wiedzą, jak zgłosić przeciążenie.	☐
16	Zapewniono dostęp do konsultacji lub superwizji.	☐
17	Ustalono sposób reagowania na agresję i groźby.	☐
18	Dostęp do systemów są nadawane według roli i odbierane po współpracy.	☐
19	Organizacja posiada sposób działania w razie awarii.	☐
20	Ustalono termin przeglądu pakietu i rejestr zmian.	☐

ZAŁĄCZNIK 7. Rejestr przeglądów i zmian

Wersja	Data	Powód przeglądu	Najważniejsze zmiany	Zatwierdził/a
0.9	2026	Projekt po diagnozie	Pierwsza kompletna wersja do konsultacji i pilotażu.	

Przy każdym przeglądzie należy sprawdzić co najmniej: wnioski z incydentów, skarg i superwizji; zmiany prawa i narzędzi; przeciążenie kadry; problemy z przekazywaniem spraw; kompletność dokumentacji; bezpieczeństwo pracy zdalnej; realność zastępstw.

Zakończenie

Pakiet ma przenieść jakość współpracy z poziomu dobrej woli i osobistego zaangażowania na poziom prostego, trwałego systemu. Nie zakłada, że mała organizacja będzie działać jak urząd lub duża placówka. Zakłada natomiast, że nawet najmniejszy zespół może jasno odpowiedzieć na siedem pytań: kto pomaga, w jakiej roli, gdzie dokumentuje, jak chroni informacje, komu zgłasza ryzyko, kto go zastępuje i jak zapewnia ciągłość pomocy.

Standard minimalny: Zweryfikowany i wdrożony specjalista, jednoznaczna odpowiedzialność, bezpieczne kanały, krótka dokumentacja, możliwość konsultacji, czytelna eskalacja oraz plan zastępstwa.

Wersja 0.9 powinna zostać poddana konsultacji Rady Społecznej ds. Standardów Współpracy, audytowi prawnemu, psychologicznemu i RODO oraz pilotażowi w organizacjach o różnej skali. Wersja 1.0 powinna zawierać rejestr uwag, odpowiedzi i zmian wynikających z walidacji.