Rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora danych

Nazwa instytucji beneficjenta oraz dane kontaktowe (do publicznego udostępnienia)		**Inspektor Ochrony Danych w instytucji beneficjenta (jeśli w instytucji beneficjenta go powołano)**	
Nazwa	Fundacja DeployingFuture	Imię i nazwisko	Michał Ochocki
Adres	Lubelska 11b, 05-071 Sulejówek	Adres	Lubelska 11b, 05-071 Sulejówek
Email	dagmara@deployingfuture.com	Email	michal@deployingfuture.com
Telefon	+48 661 939 736	Telefon	+48 666 888 799

Kategoria przetwarzania danych	**Administrator danych osobowych**			**Przekazywanie danych do krajów trzecich lub organizacji międzynarodowych** (kraj/nazwa organizacji, cel przekazania, opis zabezpieczeń)	**Opis technicznych i organizacyjnych środków bezpieczeństwa**
	Nazwa	**Adres**	**Kontakt**		
Erasmus+ i Europejski Korpus Solidarności (2021-2027): zarządzanie dotacjami i rejestracja organizacji dla działań zdecentralizowanych (https://ec.europa.eu/erasmus-esc-personal-data, DPR-EC-06826)	Komisja Europejska: Edukacja, Młodzież, Sport i Kultura (EAC)	Dyrekcja Generalna ds. Edukacji i Kultury Komisja Europejska 1049 Bruxelles/Bruksela Belgia	eu-erasmus-esc-personal-data@ec.europa.eu	Nie dotyczy – dane nie są przekazywane poza EOG	Fundacja stosuje adekwatne do poziomu ryzyka środki ochrony danych, w tym: - pseudonimizację i szyfrowanie danych osobowych (dane szczególne oraz dane wrażliwe są szyfrowane lub zabezpieczane hasłami), - środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów, - regularne testowanie i ocenę skuteczności środków zabezpieczających. Fundacja wdrożyła zasady: - czystego biurka – dokumenty zawierające dane osobowe nie mogą być pozostawione na wierzchu; po zakończeniu pracy powinny być zabezpieczone w zamkniętych szafkach lub niszczone, - czystego ekranu – obowiązek blokowania komputera za każdym razem, gdy pracownik odchodzi od stanowiska, - segmentacji dostępu – tylko osoby upoważnione mają dostęp do określonych kategorii danych, - rejestracji operacji – wszelkie operacje na danych podlegają ewidencji.

					W przypadku przetwarzania danych w formie papierowej: - dokumentacja musi być przechowywana w zamkniętej szafie pancernej, do której klucze posiadają wyłącznie osoby uprawnione, - dokumenty po wykorzystaniu muszą być niszczone w niszczarkach spełniających standardy DIN 66399 (minimum poziom P-4). Szyfrowanie stosowane jest w szczególności w odniesieniu do: - przesyłania danych osobowych drogą elektroniczną (np. za pomocą haseł do plików .zip lub za pomocą komunikatorów z szyfrowaniem end-to-end), - przechowywania baz danych z danymi wrażliwymi, - nośników zewnętrznych (np. pendrive, dyski przenośne). Komputery, serwery i urządzenia mobilne Fundacji: - zabezpieczone są hasłami z odpowiednim poziomem złożoności, - mają aktywne programy antywirusowe i zaporę sieciową, - regularnie aktualizowane systemy operacyjne i oprogramowanie. Dane są zbierane w minimalnym zakresie umożliwiającym realizację projektu. Pracownicy są zobowiązani do zachowania poufności. Dostęp do danych szczególnej kategorii mają jedynie osoby pisemnie upoważnione przez Zarząd.