Zarządzenie Nr 8/2019

Dyrektora Domu Pomocy Społecznej w Kędzierzynie-Koźlu

z dnia 19.12.2019 roku

w sprawie wprowadzenia do samooceny funkcjonowania systemu kontroli zarządczej obszaru dotyczącego ochrony danych osobowych w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

Na podstawie art. 69 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2019 poz. 869 z późn. zm.), uchwały Nr 82/397/2016 Zarządu Powiatu w Kędzierzynie -Koźlu z dnia 27.12.2016r. w sprawie zatwierdzenia Regulaminu Organizacyjnego Domu Pomocy Społecznej w Kędzierzynie-Koźlu

zarządza, co następuje:

§1

Wprowadza się do zasad dokonywania samooceny funkcjonowania systemu kontroli zarządczej w **Domu Pomocy Spolecznej w Kędzierzynie-Koźlu**, zasady dokonywania samooceny funkcjonowania systemu kontroli zarządczej w zakresie przestrzegania i realizacji Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE w Domu Pomocy Społecznej w Kędzierzynie-Koźlu, stanowiące **Załącznik Nr 1** do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
mgr inż. Ewa Sawicka

Załącznik Nr 1 do Zarządzenia Nr 8/2019
Dyrektora Domu Pomocy Społecznej w Kędzierzynie-Koźlu
z dnia 19.12.2019r.

Zasady dokonywania samooceny funkcjonowania systemu kontroli zarządczej
w zakresie RODO
w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

§ 1 Niniejszy dokument określa zasady i tryb dokonywania samooceny funkcjonowania systemu kontroli zarządczej w zakresie przestrzegania i realizacji Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanej dalej RODO) w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

§ 2 Proces samooceny jest jednym z narzędzi stosowanych w monitoringu kontroli zarządczej w Domu Pomocy Społecznej w Kędzierzynie-Koźlu, a jego celem jest uzyskanie informacji o funkcjonowaniu kontroli zarządczej w zakresie RODO.

§ 3 Samoocena w Domu Pomocy Społecznej w Kędzierzynie-Koźlu przeprowadzana jest poprzez udzielenie odpowiedzi na pytania sformułowane w kwestionariuszach. Samoocena jest wykonywana przez Kierownika Jednostki, lub osobę wyznaczoną przez Kierownika Jednostki, lub Inspektora Ochrony Danych.

§ 4 Wzory kwestionariuszy do przeprowadzenia samooceny funkcjonowania systemu kontroli zarządczej w zakresie RODO w Domu Pomocy Społecznej w Kędzierzynie-Koźlu stanowią **Załączniki Nr 1, Nr 2, Nr 3, Nr 4** do niniejszych zasad.
Kwestionariusze samooceny dotyczą:

1) zasad wyznaczania inspektora ochrony danych,
2) zasobów niezbędnych do wprowadzenia i funkcjonowania RODO,
3) zadań inspektora ochrony danych,
4) rozliczalności z zakresu wdrożonych polityk, procedur i instrukcji postępowania w zakresie przestrzegania RODO

§ 5 Termin przeprowadzenia samooceny funkcjonowania systemu kontroli zarządczej w zakresie RODO **w** Domu Pomocy Społecznej w Kędzierzynie-Koźlu ustala się **do 30 kwietnia każdego roku**. Wypełnione kwestionariusze w formie papierowej, należy przedłożyć u Kierownika Jednostki

§ 6 Dokumentem potwierdzającym przeprowadzenie Samooceny w zakresie RODO w Domu Pomocy Społecznej w Kędzierzynie-Koźlu jest Raport z dokonanej samooceny wykonany przez Kierownika Jednostki, osobę wyznaczoną przez Kierownika Jednostki, lub przez Inspektora ochrony danych. Przeprowadzana corocznie samoocena dotyczy zawsze roku ubiegłego.

§ 7 1.Wyniki samooceny są podstawą do pisemnego Raportu zawierającego co najmniej następujące informacje:

1) cel przeprowadzonej samooceny,
2) zakres samooceny przedmiotowy i podmiotowy,
3) wyniki samooceny: ogólna ocena stanu kontroli zarządczej, zidentyfikowane ryzyka, słabości kontroli zarządczej, proponowane działania naprawcze.

2. Wzory kwestionariuszy / ankiet wykorzystane w procesie samooceny dołącza się do raportu.

§ 8 Za sporządzenie Raportu zbiorczego z przebiegu procesu samooceny w zakresie RODO w Domu Pomocy Społecznej w Kędzierzynie-Koźlu odpowiedzialny jest Kierownik Jednostki w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

Załącznik Nr 1 do Zasad dokonywania samooceny
funkcjonowania systemu kontroli zarządczej w zakresie RODO
w **Domu Pomocy Społecznej w Kędzierzynie-Koźlu**

Zasady wyznaczania inspektora ochrony danych
w Domu Pomocy Społecznej w Kędzierzynie-Koźlu wg stanu na dzień ..... 2019 r.

L p.	Zasady	Tak	Nie	Uwagi
1	2	3	4	5
1	Brak konfliktu interesów, inspektor ochrony danych nie zajmuje: - stanowiska kierowniczego - stanowiska biorącego udział w określaniu celów i sposobów przetwarzania danych	[x]	[ ]	
2	Zidentyfikowane zostały stanowiska niekompatybilne z funkcją inspektora ochrony danych	[x]	[ ]	
3	Obowiązują wewnętrzne zasady uniemożliwiające łączenie stanowisk będących w konflikcie interesów	[x]	[ ]	
4	Stanowisko inspektora ochrony danych zapewnia, że: - przedstawiona oferta świadczenia usług lub ogłoszenie o rekrutacji na stanowisko IOD jest wystarczająco jasne i precyzyjne - umowy o świadczenie usług są wystarczająco jasne i precyzyjne - przyjęte zasady powołania IOD niwelują ryzyko powstania konfliktu interesów	[x]	[ ]	
5	Określone są niezbędne kwalifikacje dla inspektora ochrony danych: - wiedza na temat krajowych i europejskich przepisów i praktyk w zakresie ochrony danych - rozumienie przeprowadzanych procesów przetwarzania - rozumienie technologii informacyjnych i bezpieczeństwa danych - umiejętność promowania kultury ochrony danych w jednostce	[x]	[ ]	

Sporządził, dnia ..... 2019 r. Zatwierdził, dnia .....
(data i podpis kierownika jednostki)

Załącznik Nr 2 do Zasad dokonywania samooceny
funkcjonowania systemu kontroli zarządczej
w zakresie RODO
w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

Zasoby niezbędne do wprowadzenia i funkcjonowania RODO
w Domu Pomocy Społecznej w Kędzierzynie-Koźlu stan na dzień ..... 2019 r.

Lp.	Zasoby niezbędne	Istniejące zasoby w jednostce		Termin wykonania	Komórka organizacyjna	Osoba odpowiedzialna	Uwagi
		Tak	Nie				
1	2	3	4	5	6	7	8
1	Odpowiednie wsparcie kadrowe	[x]	[ ]				
2	Współpraca osób zatrudnionych przy przetwarzaniu danych z inspektorem ochrony danych	[x]	[ ]				
3	Sprzęt i wyposażenie niezbędne do prawidłowego przetwarzania danych oraz zabezpieczenia danych osobowych	[x]	[ ]				
4	Zabezpieczenie finansowe odpowiednie do zakresu przetwarzanych danych	[x]	[ ]				
5	Umożliwienie inspektorowi ochrony danych dostępu do wszystkich niezbędnych działów organizacji	[x]	[ ]				
6	Wystarczająca wiedza pracowników na temat RODO	[x]	[ ]				
7	Poinformowanie pracowników o wyznaczeniu inspektora ochrony danych i zadaniach, jakie wykonuje	[x]	[ ]				
8	Zabezpieczenie inspektorowi ochrony danych pełnego dostępu do danych osobowych i operacji przetwarzania	[x]	[ ]				
9	Wsparcie dla inspektora ochrony danych ze strony kadry kierowniczej	[x]	[ ]				

Sporządził, dnia ..... 2019 r. Zatwierdził, dnia .....
(data i podpis kierownika jednostki)

Załącznik Nr 3 do Zasad dokonywania samooceny
funkcjonowania systemu kontroli zarządczej w zakresie RODO
w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

Zadania inspektora ochrony danych w Domu Pomocy Społecznej w Kędzierzynie-Koźlu wg stanu na dzień ..... 2019 r.

Lp.	Rodzaj zadania	Tak	Nie	Uwagi
1	2	3	4	5
1	Monitorowanie przestrzegania RODO: - zbieranie informacji w celu identyfikacji procesów przetwarzania - analizowanie i sprawdzanie zgodności przetwarzania - informowanie, doradzanie i rekomendowanie określonych działań administratorowi albo podmiotowi przetwarzającemu	[x]	[ ]	
2	Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych i doradzanie im w tej sprawie	[x]	[ ]	
3	Ocena skutków dla ochrony danych: - systematyczny opis planowanych operacji przetwarzania oraz celów przetwarzania - określenie metodologii do przeprowadzenia oceny skutków dla ochrony danych - ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów - ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą - wskazanie, jakie zabezpieczenia (w tym środki techniczne i organizacyjne) mają zastosowanie w celu złagodzenia wszelkich zagrożeń dla praw i interesów osób, których dane dotyczą - wskazanie, czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu - ustalenie, czy ocena skutków została prawidłowo przeprowadzona oraz czy jej wyniki są zgodne z wymogami ochrony danych (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować)	[x]	[ ]	
4	Udzielanie, na żądanie, zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania	[x]	[ ]	
5	Współpraca z organem nadzorczym	[x]	[ ]	
6	Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz prowadzenie konsultacji we wszelkich innych sprawach	[x]	[ ]	
7	Prowadzenie, w imieniu administratora albo podmiotu przetwarzającego, rejestru czynności przetwarzania danych	[x]	[ ]	
8	Wykonywanie zadań z uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania, podejście oparte na analizie ryzyka	[x]	[ ]	

9	Wskazywanie: - jakie szkolenia wewnętrzne przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych - na które operacje przetwarzania przeznaczyć więcej czasu i zasobów	[x]	[ ]	
10	Wsparcie ze strony IOD w zakresie przeprowadzenia analizy ryzyka i oceny skutków dla ochrony danych	[x]	[ ]	

Sporządził, dnia ..... 2019 r. Zatwierdził, dnia ....

(data i podpis kierownika jednostki)

Załącznik Nr 4 do Zasad dokonywania samooceny
funkcjonowania systemu kontroli zarządczej w zakresie RODO
w Domu Pomocy Społecznej w Kędzierzynie-Koźlu

Rozliczalność z zakresu wdrożonych polityk, procedur i instrukcji postępowania w zakresie przestrzegania RODO w Domu Pomocy Społecznej w Kędzierzynie-Koźlu stan na dzień ..... 2019 r.

Lp.	Zasoby niezbędne	Istniejące zasoby w jednostce		Termin wykonania	Komórka organizacyjna	Osoba odpowiedzialna	Uwagi
		Tak	Nie				
1	2	3	4	5	6	7	8
1	Wdrożenie odpowiednich środków organizacyjno – technicznych o których mowa w art. 32 RODO	[x]	[ ]				
2	Wykonanie obowiązków administratora o których mowa w art. 24 RODO	[x]	[ ]				
3	Realizacja obowiązku wynikającego z art. 28 RODO poprzez zawieranie pisemnych umów powierzenia przetwarzania z podmiotami zewnętrznymi w przypadku konieczności przekazania im danych osobowych	[x]	[ ]				
4	Odpowiednie zapisy w umowach na świadczenie usług dających gwarancję poufności danych (SLA)	[x]	[ ]				
5	Wdrożenie polityk i procedur postępowania w przypadku przetwarzania danych	[x]	[ ]				
6	Prowadzenie rejestrów o których mowa w art. 30 ust. 1 i 2 RODO	[x]	[ ]				
7	Dokumentowanie wszelkich naruszeń ochrony danych osobowych zgodnie z art. 33 ust. 5 RODO - prowadzenie rejestru incydentów i naruszeń	[x]	[ ]				
8	Przeprowadzanie analizy ryzyka	[x]	[ ]				
9	Realizacja obowiązku informacyjnego o którym mowa w art. 13 RODO	[x]	[ ]				
10	Przeprowadzanie audytu bezpieczeństwa informacji	[x]	[ ]				
11	Realizacja wytycznych Rozporządzenia KRI	[x]	[ ]				
12	Wydawanie i aktualizacja upoważnień do przetwarzania danych osobowych						

Sporządził, dnia ..... 2019 r. Zatwierdził, dnia .....

(data i podpis kierownika jednostki)