

ZARZĄDZENIE NR 128. 2020

**Wójta Gminy Odrzywół
z dnia 30 czerwca 2020 roku**

**w sprawie wprowadzenia Dokumentacji oceny skutków dla ochrony danych osobowych
w Urzędzie Gminy w Odrzywole**

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U.2020.713), w związku z Motywem 84 Preambuły oraz art. 35 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 (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE.L.2016.119.1), zarządzam co następuje:

§ 1. Wprowadza się w Urzędzie Gminy w Ocena skutków przetwarzania dla ochrony danych osobowych stanowiącą załącznik Nr 1 do niniejszego Zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

W O J T
mgr Marian Kmiecik

**OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA)
MONITORING****Nazwa i dane kontaktowe administratora**

Nazwa	URZĄD GMINY W ODRZYWOLE
Adres	26-425 Odrzywół, ul. Warszawska53
Email	sektretariat@odrzywol.eu
Telefon	48 6716057

Inspektor Ochrony Danych

Nazwa	Ilona Głogowska-Kowalczyk
Adres	26-600 Radom, ul. Żwirki i Wigury 40 Lok. 23
Email	kancelaria.odo@gmail.com
Telefon	608292823
Wersja:	Pierwsza wersja dokumentu
Data wersji:	20 maja 2020r.
Zatwierdzony przez:	Marian Kmiecniak-Wójt Gminy Odrzywół

Historia zmian

Data:	20.05.2020r.
Wersja:	0.1
Utworzona przez:	Ilona Głogowska-Kowalczyk
Opis zmian:	Pierwsza wersja dokumentu
Dokumenty powiązane:	Regulamin monitoringu wizyjnego, Szacowanie ryzyka dla ochrony danych osobowych, Rejestr czynności przetwarzania danych osobowych.

1. DECYZJA O PRZEPROWADZENIU DPIA

Opis czynności przetwarzania danych osobowych:	Uzasadnienie przeprowadzenia DPIA
Prowadzenie monitoringu wizyjnego na terenie Gminy Odrzywól.	<p><u>Na podstawie wytycznych Grupy Roboczej art. 29 oraz art. 35 ust. 3 lit. c RODO</u></p> <p>- Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie” art. 35 lit. c. Ten rodzaj monitorowania stanowi jedno z kryteriów, ponieważ dane osobowe mogą być gromadzone w sytuacji, gdy osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub w przestrzeni publicznie dostępnej).</p>

2. IDENTYFIKACJA INTERESARIUSZY , OKREŚLENIE POTRZEB W ZAKRESIE KONSULTACJI I SPORZĄDZENIE ICH PLANU

Interesariusz	Zagadnienia do konsultacji
Mieszkańcy Podróżni Interesanci UG Pracownicy Policja Serwisanci	Zasadność wprowadzenia monitoringu

3. OPIS ZAKRESU OCENY

3.1 Informacje ogólne:

1.	Proces dotyczący przetwarzania PII/system informatyczny przetwarzający PII	Monitoring wizyjny. Dostęp do systemu za pomocą strony www
2.	Cel przetwarzania PII	Zapewnienie bezpieczeństwa osób, ochrona mienia

3.	Kategorie osób, których dane dotyczą	Mieszkańcy Podróźni Interesanci GM Pracownicy Policja Serwisanci			
4.	Kategorie PII-planowany zakres danych identyfikujących osobę fizyczną (PII), który będzie przetwarzany	Dane wizerunkowe			
5.	Czy w zakresie przetwarzanych danych znajdują się szczególne kategorie danych	Nie			
6.	Odbiorcy PII i sposób wykorzystania przez nich PII	Nazwa odbiorcy	Kategoria odbiorcy	Zakres PII	Cel udostępnienia PII i sposób wykorzystania PII przez odbiorcę
		Policja, ubezpieczyciele Dostawca usług-serwis	Administrator, podmiot przetwarzający, strona trzecia	Dane wizerunkowe	Policja, ubezpieczyciele w ramach prowadzonych czynności, osoby występujące z wnioskiem o udostępnienie, na podstawie zgody Administratora Danych
7.	Okres retencji danych	3 m-ce			
8.	Przepis prawa, umowy i inne zobowiązania warunkujące przetwarzanie danych; Podstawa prawna przetwarzania PII	Art. 6 ust.1 lit. c ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016r., art.9a ust. 1 ustawy z dn. 8 marca 1990r. o samorządzie gminnym (Dz.U.2020.713 t.j.), art. 114 ustawy z dn. 10 maja 2018r. o ochronie danych osobowych (Dz.U.2019.1781 t.j.). Regulamin monitoringu wizyjnego.			
9.	Korzyści oferowane podmiotowi PII	Bezpieczeństwo			

w związku z przetwarzaniem danych w tym procesie przez Administratora Danych	
--	--

3.2 opis planowanego sposobu/procesu realizacji praw podmiotów PII:

I.p.	Prawo podmiotu PII	Opis planowanego sposobu realizacji
1.	Realizacja obowiązku informacyjnego art. 13-14 RODO	Piktogramy, pełna klauzule informacyjna znajduje się na stronie BIP, regulamin monitoringu dostępny u Sekretarza UG
2.	Zapewnienie swobodnego wyrażania zgody art. 7 RODO	Nie dotyczy
3.	Zapewnienie możliwości wyrażenia sprzeciwu art. 21-22 RODO	Nie dotyczy
4.	Zapewnienie możliwości dostępu do danych art. 15 RODO	Dostęp do swoich danych po zwróceniu się do IOD lub ASI
5.	Zapewnienie możliwości sprostowania art. 16 RODO	Nie dotyczy
6.	Zapewnienie prawa do usunięcia PII art. 17 RODO	Po upływie 3 m-cy lub po zakończeniu postępowania
7.	Zapewnienie możliwości ograniczenia przetwarzania art. 18 RODO	Dostęp do swoich danych po zwróceniu się do IOD lub ASI, na podstawie przesłanek dopuszczalności ograniczenia przetwarzania
8.	Zapewnienie możliwości przeniesienia danych art. 20 RODO	Nie dotyczy

3.3 identyfikacja i opis aktywów wspierających przetwarzanie PII

Systemy informatyczne wspierające analizowany proces				
Nazwa systemu lub jego komponentu	Lokalizacja systemu z uwzględnieniem jego głównych komponentów	Określenie kto w jakim celu i zakresie będzie mógł mieć dostęp do poszczególnych komponentów	Do jakich innych systemów opisywany system będzie przesyłał PII i w jakim zakresie	Jaki zakres PII będzie znajdował się w systemie i kiedy będzie on usuwany
System monitoringu wizyjnego	Kamery, serwer, stacje robocze	Administrator danych	Poczta elektroniczna, urządzenia mobilne	Dane wizerunkowe, usuwane najpóźniej po upływie 3 m-cy

Kanały transmisji PII				
	Dedykowane łącza informatyczne o dostępie ograniczonym dla innych podmiotów	Publiczna sieć informatyczna	Telefonia komórkowa	Inne
Pomiędzy podmiotem PII a ADO	Tak	Nie	Tak	Nie
Pomiędzy podmiotem PII a podmiotem przetwarzającym	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Pomiędzy podmiotem PII a stroną trzecią	Nie	Nie	Nie	Udostępnienie nagrania na podstawie wniosku i zgody ADO
Pomiędzy podmiotem przetwarzającym a ADO	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Pomiędzy podmiotem przetwarzającym a stroną trzecią	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy
Pomiędzy różnymi ADO	Tak	Tak	Nie	Płyta CD
Inne	-	-	-	-

3.4 opis operacji przetwarzania PII

Cykl życia danych	Opis
Zbieranie. Sposób zbierania danych (z jakich źródeł, jakimi kanałami).	Dane pochodzą bezpośrednio od osób, których dotyczą
Przechowywanie. W jakich zasobach będą przechowywane dane (serwery, stacje robocze, metalowe szafy, zamykane biurka itp.).	Przechowywane na stacji bezpośrednio w miejscu nagrywania. Możliwość odbioru na nośnikach zewnętrznych, zgrywania oraz przechowywania na CD.
Używanie. W jaki sposób będą wykorzystywane dane, jakie operacje będą na nich wykonywane (w szczególności czy będą profilowane, łączone, czy będą podejmowane decyzje w sposób zautomatyzowany, czy będą porównywane).	Wykorzystywane w sytuacji wyrządzenia krzywdy lub szkody.
Przekazywanie. Które podmioty zewnętrzne	Policja w trakcie czynności operacyjnych

będą miały możliwość dostępu do danych niezależnie od postaci w jakiej te dane będą przekazywane ani od roli podmiotu zewnętrznego (inny ADO, podmiot. przetwarzający) W jakim celu i w jakim zakresie dane będą przekazywane podmiotom zewnętrznym	lub na wniosek, sąd, prokuratura, podmiot, który wystąpi z wnioskiem o udostępnienie zgodnie z wewnętrzną procedurą urzędu, jeżeli ADO wyda zgodę.
Usuwanie. W jakich okolicznościach, na czyj wniosek będą usuwane dane, w jakim zakresie i z jakich zasobów.	Po 3 miesiącach lub po zakończeniu postępowania w sprawie.

4. USTALENIE ISTOTNYCH WYMOGÓW W ZAKRESIE OCHRONY PRYWATNOŚCI I OCENA ZGODNOŚCI

Wymagania w zakresie ochrony prywatności	Dodatkowe informacje dotyczące sposobu realizacji	Ocena zgodności przedmiotu DPIA z wymogami w zakresie ochrony prywatności (ocena IOD)	Działania wymagane w celu zapewnienia zgodności
Ogólne zasady prywatności (ISO/IEC 29100)			
Zgoda i wybór	n/d	n/d	n/d
Legalność i określenie celów	art.9a ust. 1 ustawy z dn. 8 marca 1990r. o samorządzie gminnym (Dz.U.2020.713 t.j.), art.114 ustawy z dn. 10 maja 2018r.o ochronie danych osobowych (Dz.U.2019.1781 t.j).	Zgodne Cele zgodne z obowiązującym prawem Podmioty PII poinformowane odpowiednimi klauzulami	Zgodne
Ograniczanie zbierania	Zakres danych ograniczony do tych, które mieszczą się w granicach wyznaczonych przez obowiązujące prawo oraz są bezwzględnie niezbędne do realizacji wyznaczonych celów	Zgodne	Zgodne
Minimalizacja danych	Wykorzystanie danych w minimalnym zakresie, wyłącznie danych wizerunkowych niezbędnym do osiągnięcia celów ADO tj. zapewnienia bezpieczeństwa	Zgodne Ograniczony dostęp do danych, wyłącznie dla upoważnionego pracownika oraz w uzasadnionych przypadkach na wniosek, po upływie max. 3 m-cy dane są usuwane	Zgodne
Ograniczanie używania, zatrzymywania i ujawniania	Określony czas retencji danych do 3 m-cy, dane zatrzymywane wyłącznie tak długo jak jest to konieczne do realizacji podanego celu, a następnie są bezpiecznie usuwane	Zgodne	Zgodne
Dokładność i jakość	Wynika z technologii i założeń systemu	Zgodne Przetwarzane dane są	Należy wprowadzić mechanizmy

	monitoringu	kompletne, adekwatne i istotne dla celu, zasady prowadzenia monitoringu określono w Regulaminie stosowania monitoringu wizyjnego	kontroli w celu okresowego sprawdzania dokładności i jakości zebranych i przechowywanych danych
Otwartość, przejrzystość i zawiadamianie	Podmiotom PII przekazano klauzule informacyjne, w miejscach objętych monitoringiem znajdują się oznakowania	Zgodne	Zgodne
Indywidualne uczestnictwo i dostęp	Podmiotom umożliwiono o dostęp do ich PII pod warunkiem uprzedniego potwierdzenia tożsamości z odpowiednią pewnością oraz pod warunkiem, że taki dostęp nie jest zabroniony, wprowadzono procedury umożliwiające podmiotom PII proste, szybkie i skuteczne wykonywanie swoich praw - bez zbędnej zwłoki i nieuzasadnionych kosztów	Zgodne	Zgodne
Odpowiedzialność	ADO wprowadził Regulamin monitoringu wizyjnego, podmiot PII może kontaktować się w sprawie swoich danych z IOD oraz ASI, organizowanie szkoleń dla pracowników ADO, którzy będą mieć dostęp do PII	Zgodne	Zgodne
Bezpieczeństwo informacji	Ograniczenie dostępu do PII, przysługuje on tylko osobom, którym taki dostęp jest potrzebny w celu wykonywania swoich obowiązków, eliminowanie ryzyk i słabych punktów podczas audytów, poddawanie systemu okresowym przeglądom	Zgodne	Zgodne
Zgodność z zasadami prywatności	Okresowe audyty, przeprowadzenie badania ryzyka	Zgodne	Zgodne
Inne zidentyfikowane wymagania w zakresie ochrony prywatności			
-	-	-	-

5. SZACOWANIE RYZYKA DLA PRYWATNOŚCI

Na podstawie (ISO/IEC 27005)

I.p.	Źródło zagrożenia	Ryzyko	Zagrożenie	Podatności	Skutek dla podmiotu PII	Wartość skutku *	Wartość prawdopodobieństwa**
1.	Pracownicy wewnątrz organizacji	Utrata poufności	Niepożądana modyfikacja danych, usunięcie, kopiowanie, ujawnienie, błąd użytkownika, kradzież nośników, nielegalne przetwarzanie danych	Zakłada się ograniczoną skuteczność stosowanych szkoleń z bezpieczeństwa; Zakłada się ograniczoną skuteczność stosowanych rozwiązań pod względem zabezpieczeń co w fazie eksploatacji systemu może doprowadzić do naruszenia prywatności	Naruszenie poufności	2	1
2.	Awarie sprzętu i oprogramowania	Utrata integralności i dostępności	Niewłaściwe funkcjonowanie sprzętu, zniszczenie urządzeń	Brak planów okresowej wymiany	Naruszenie dostępności	1	1

*Skala skutku/oddziaływanie:

1. Pomijalne
2. Ograniczone
3. Istotne
4. Maksymalne

****Skala prawdopodobieństwa:**

1. Pomijalne
2. Ograniczone
3. Istotne
4. Maksymalne

SKALA POZIOMU RYZYKA	WARTOŚĆ (R=P*S)
ryzyko akceptowane	1-4
ryzyko o maksymalnej wartości skutku i pomijalnym prawdopodobieństwie mogą zostać zaakceptowane pod warunkiem spełnienia wymogów zgodności po ustaleniu czy korzyści przeważają nad ryzykami dla podmiotu PII	4
ryzyko jest nieakceptowalne Należy ustalić czy ryzyka dla podmiotu PII przeważają nad korzyściami w takim przypadku należy zastosować środki zmniejszające ryzyko	6-16

6. WYBÓR OPCJI POSTĘPOWANIA Z RYZYKIEM ORAZ DOBÓR MECHANIZMÓW KONTROLI

l.p.	Wybór opcji postępowania: akceptacja, unikanie, przeniesienie, zmniejszenie	Proponowany mechanizm kontrolny
1.	Akceptacja	Audyt wewnętrzny, kontrola serwisowa raz w roku

7. DECYZJA O POTRZEBIE KONSULTACJI Z ORGANEM NADZORCZYM

Wobec zdiagnozowania ryzyka na poziomie dla ADO akceptowalnym, brak konieczności konsultacji z organem nadzorczym.

8. PLAN POSTĘPOWANIA Z RYZYKIEM

Dotyczy: systemu monitoringu wizyjnego na terenie Gminy Odrzywół

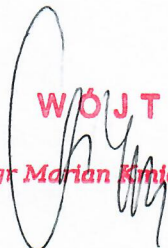
Kategorie PII- planowany zakres danych identyfikujących osobę fizyczną, który będzie przetwarzany	Dane wizerunkowe

Zadanie/projekt do wykonania	Zasoby ludzkie wymagane do realizacji zadania/projektu	Inne zasoby wymagane do realizacji	Osoba odpowiedzialna za projekt	Termin realizacji	Zasady monitorowania i raportowania postępu realizacji
Aktualizacja oprogramowania	Zlecenie podmiotowi przetwarzającemu	-	ADO	Grudzień 2021r.	Raport dostawcy oprogramowania

Szkolenia z zakresu bezpieczeństwa danych	Szkolenie wewnątrz organizacji	-	IOD	Maj 2021r.	Plan przeprowadzenia szkolenia, ankiety uczestników, testy znajomości zasad i procedur ochrony danych osobowych
---	--------------------------------	---	-----	------------	---

9.RAPORT Z DPIA

Dla podmiotów PII kluczowe są korzyści płynące z możliwości zapewnienia bezpieczeństwa osób oraz mienia, w systemie przetwarzane będą wyłącznie dane wizerunkowe podmiotów PII, w analizie wykazano podstawy prawne stosowania monitoringu wizyjnego, zapewniono gwarancje bezpieczeństwa przetwarzanych danych wizerunkowych, organizacja wdroży plan cyklicznego przeprowadzania przeglądów serwisowych systemów, podmiotom PII zapewniono możliwość dostępu do ich danych oraz spełniono wobec nich obowiązek informacyjny, dostępność klauzuli na stronie bip UG, podano do wiadomości dane kontaktowe IOD, oraz dane ADO.


WÓJT
mgr Marian Kmiecik