

Zarządzenie Nr 36/2018
Wójta Gminy Kroczyce
z dnia 24 maja 2018 r.

w sprawie: wprowadzenia „Polityki ochrony danych” w Urzędzie Gminy Kroczyce

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tj. Dz. U. z 2018r., poz. 994) oraz art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, L119 z 4.05.2016 t.)

zarządzam, co następuje:

§ 1.

Wprowadza się „Politykę ochrony danych w Urzędzie Gminy Kroczyce”, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie Zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania


WÓJTA
inż. Stefan Pantak

Polityka Ochrony Danych Osobowych w Urzędzie Gminy Kroczyce

1	Wstęp	1
2	Ocena skutków (analiza ryzyka).....	2
2.1	Opis operacji przetwarzania (inventaryzacja aktywów).....	2
2.2	Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)	2
2.3	Analiza ryzyka.....	2
2.4	Plan postępowania z ryzykiem	4
3	Upoważnienia	4
4	Instrukcja postępowania z incydentami	4
5	Regulamin Ochrony Danych Osobowych.....	5
6	Rejestr czynności przetwarzania.....	5
7	Wykaz zabezpieczeń	5

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

2.1 OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku 01. Rejestr czynności przetwarzania jako zbiór danych.
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
 - a. opis kategorii osób (nazwę zbioru)
 - b. opis celów przetwarzania
 - c. charakter, zakres, kontekst danych osobowych
 - d. odbiorcy danych
 - e. funkcjonalny opis operacji przetwarzania
 - f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing)

2.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator przetwarzający dane osobowe (patrz 01. Rejestr czynności przetwarzania jako zbiór danych) zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności należy zapewnić, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9)
2. dane te są adekwatne w stosunku do celów przetwarzania
3. dane te są przetwarzane przez określony czas (retencja danych)
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody)
5. opracowano klauzule informacyjne dla powyższych osób (patrz załącznik 02. Klauzule informacyjne)
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28).

2.3 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania.

2.3.1 Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (Incident) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

3. Zagrożenie - potencjalne naruszenie (potencjalny incydent)
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

2.3.2 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, lub w procesie przetwarzania
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów

2.3.3 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: $R = P * S$

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.3.4 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.3.5 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
 - a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
 - b. Unikanie – eliminacja działań powodujących ryzyko

3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka
4. Analizę ryzyka przeprowadza się w specjalnym szablonie (programie) 02e Arkusz analizy ryzyka RODO

2.3.6 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne)

2.4 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są w formie papierowej.

4 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych)
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
 - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
 - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
 - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
 - a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
 - b. inicjuje ewentualne działania dyscyplinarne
 - c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
 - d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze –patrz załącznik [03 Formularz rejestracji incydentu](#)
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik - [04 Regulamin Ochrony Danych Osobowych](#)

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności.

6 REJESTR CZYNNOŚCI PRZETWARZANIA

1. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia 01. Rejestr czynności przetwarzania jako zbiór danych)

7 WYKAZ ZABEZPIECZEŃ

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik Instrukcja zarządzania RODO/
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne
3. Instrukcja / wykaz jest aktualizowana po każdej ocenie skutków.


WÓJT
inż. Stefan Pantak