

**ZARZĄDZENIE Nr 0050<sup>99</sup>...2019**  
**Burmistrza Czerwieńska**  
**z dnia 04 września 2019 r.**

**w sprawie wprowadzenia „Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”**

Na podstawie art. 24 ust 1 i 2 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 119/1), **zarządza się, co następuje:**

§ 1. Wprowadza się „Politykę Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”, która stanowi załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się członków Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku, do realizacji niniejszego zarządzenia.

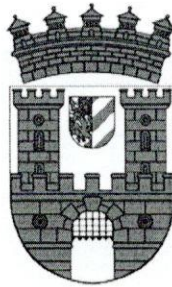
§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

**BURMISTRZ**  
*Piotr Iwanus*

**RADCA PRAWNY**  
*mgr Justyna Prętkowska*  
12/ZG

Załącznik do zarządzenia nr 0050.99.2019  
Burmistrza Czerwińska  
z dnia 04 września 2019 r.

# **POLITYKA BEZPIECZEŃSTWA**



## **DOTYCZĄCA OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH**

### **GMINNEJ KOMISJI ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH W CZERWIEŃSKU**

---

Czerwińsk 2019 r.

## **1. POSTANOWIENIA WSTĘPNE**

§ 1. Gminna Komisja Rozwiązywania Problemów Alkoholowych w Czerwieńsku, zwana dalej Komisją, przetwarza dane osobowe w celu realizacji zadań, do których została utworzona, a które są określone w ustawie o wychowaniu w trzeźwości i przeciwdziałania alkoholizmowi oraz regulaminie Komisji.

§ 2. Zapewnienie wysokiego standardu ochrony danych osobowych należy do priorytetów Komisji.

## **2. WYKAZ MIEJSC TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE**

### **Wykaz budynków:**

1. Budynek Urzędu Gminy i Miasta w Czerwieńsku przy ul. Rynek 25, 66-016 Czerwieńsk
2. Punkt Konsultacyjno – Terapeutyczny zlokalizowany w budynku Miejsko-Gminnej Biblioteki Publicznej w Czerwieńsku przy ul. Bolesława Chrobrego 2, 66-016 Czerwieńsku

## **3. WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW DO ICH PRZETWARZANIA**

Wykaz zbiorów danych osobowych:

- Teczki osobowe z zawartością wszystkich dokumentów otrzymanych i wytworzonych podczas prowadzenia postępowania wobec zgłoszonej osoby nadużywającej alkoholu i innych środków odurzających.
- Rejestr pism przychodzących oraz wychodzących i wytworzonych w formie papierowej.

## **4. ŚRODKI BEZPIECZEŃSTWA**

### **➤ Środki Organizacyjne:**

§ 1. Nadzór nad przestrzeganiem zasad ochrony danych osobowych oraz danych wrażliwych sprawuje Przewodnicząca/-y/ Komisji.

§ 2. 1. Do przetwarzania danych osobowych oraz danych wrażliwych dopuszcza się jedynie członków Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku, którzy podpisują stosowne oświadczenia o zachowaniu w tajemnicy dotyczącej danych osobowych.

2. Do przetwarzania danych osobowych w systemie informatycznym, dopuszcza się jedynie Przewodniczącą/-ego/ Komisji.

§ 3. Każda osoba upoważniona do przetwarzania danych osobowych (członkowie Komisji) ma obowiązek zapoznać się z ustawą *o ochronie danych osobowych*

w aktualnym brzmieniu oraz Rozporządzeniem 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 119/1), Polityką Bezpieczeństwa Gminnej Komisji Rozwiązywania Problemów Alkoholowych oraz regulaminem Komisji.

§ 4. 1. Członkowie Komisji mają szczególny obowiązek dbania o to, aby podczas wizyty osób trzecich oraz podczas posiedzeń Komisji, nie doszło do naruszenia ochrony danych osobowych.

2. W celu zapewnienia obowiązku z ust. 1 zapewnia się następujące środki bezpieczeństwa:

- monitor komputera musi być tak ustawiony, aby uniemożliwiało to dostęp do wyświetlania danych osób nieuprawnionych;
- dane osobowe nie przetwarzane za pomocą komputera muszą być tak przechowywane, aby w przypadku wizyty osób trzecich nie miały one możliwości zapoznania się z informacjami, do których nie są uprawnione; w szczególności realizacja tego obowiązku polega na odkładaniu akt sprawy w bezpieczne miejsce do tego przeznaczone zaraz po skończeniu z nimi pracy, na biurku powinny znajdować się tylko akta sprawy, nad która aktualnie się pracuje;
- nakazuje się przeprowadzanie rozmów w sposób uniemożliwiający naruszenie ochrony danych osobowych.

§ 5. Po zakończeniu pracy należy zabezpieczyć wszystkie materiały, zawierające dane osobowe przed dostępem osób nieuprawnionych.

§ 6. Dokumentacja zawierająca dane osobowe może znaleźć się poza obszarem przetwarzania danych osobowych, określonych w wykazie miejsc przetwarzania danych, tylko w szczególnych przypadkach. Za takie przypadki uważa się np. konsultacje z radcą prawnym itp.

➤ **Środki Techniczne:**

§ 7. Fizyczne środki ochrony danych: zamki w szafach, alarm w budynku Urzędu Gminy i Miasta w Czerwieńsku.

§ 8. Środki ochrony w ramach oprogramowania systemów: hasło użytkownika, program antywirusowy.

## 5. KORESPONDENCJA

§ 1. Korespondencję zaadresowaną do Gminnej Komisji Rozwiązywania Problemów Alkoholowych przyjmuje Sekretariat Urzędu przybijając pieczęć wpływu do Urzędu Gminy i Miasta w Czerwieńsku, a następnie tak przygotowaną i zamkniętą

korrespondencję przekazuje do Przewodniczącej/-ego/ lub Sekretarza Komisji, którzy prowadzą w tym celu odrębną ewidencję.

§ 2. Przewodnicząca/-y/ Komisji lub Sekretarz Komisji ewidencjonuje korespondencję w celu jej dalszego przetwarzania.

### **3. POSTANOWIENIA KOŃCOWE**

§ 1. Osoba, której dane osobowe są przetwarzane ma prawo do kontroli danych jej dotyczących, a zwłaszcza do uzyskania następujących informacji:

- Jakie dane osobowe zawiera zbiór;
- W jaki sposób zabrano dane;
- Od kiedy przetwarza się dane w zbiorze;
- Czy dane osobowe zostały udostępnione innym podmiotom i na jakiej podstawie prawnej

**Ponadto:**

- Kto jest Administratorem Danych Osobowych;
- Kto jest Inspektorem Ochrony Danych;
- Cel przetwarzania jego danych osobowych;
- Podstawa prawna przetwarzania jego danych osobowych;
- Okres przechowywania jego danych osobowych;
- Kto jest odbiorcą jego danych osobowych;
- Jakie ma prawa związane z przetwarzaniem danych osobowych;
- W jaki sposób może wnieść skargę w przypadku nieprawidłowości przy przetwarzaniu jego danych osobowych;
- Jakie dane zawiera

§ 2. W razie naruszenia zasad ochrony danych osobowych klientów Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku stosuje się procedury określone w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.

#### **Załączniki do Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku:**

1. Oświadczenie o zachowaniu tajemnicy dotyczącej danych osobowych.
2. Oświadczenie o zachowaniu poufności informacji i danych.
3. Upoważnienie do przetwarzania danych osobowych i danych wrażliwych.
4. Oświadczenie o zapoznaniu się z regulaminem Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku.
5. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.
6. Dziennik korespondencji przychodzącej
7. Dziennik korespondencji wychodzącej

Załącznik 1 do Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”

Czerwieńsk, dnia ..... r.

.....  
(imię i nazwisko )

.....

.....  
(adres zamieszkania)

### **OŚWIADCZENIE o zachowaniu tajemnicy dotyczącej danych osobowych**

Jako członek Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku, w związku z koniecznością wykonywania zadań określonych w ustawie o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, zobowiązuję się do zachowania w tajemnicy, danych osobowych przetwarzanych przez Komisję.

.....  
(czytelny podpis )

Załącznik 2 do Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”

Czerwieńsk, dnia ..... r.

.....  
(imię i nazwisko )

.....  
(stanowisko w GKRPA)

.....

.....  
(adres zamieszkania)

## **BURMISTRZ CZERWIĘŃSKA**

Na podstawie art. 25 a ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałania alkoholizmowi (Dz. U. z 2018 r. poz. 2137 z późn. zm.)

### **OŚWIADCZAM**

że zachowam poufność informacji i danych, które uzyskałem/-am/ przy realizacji zadań związanych z procedurą zobowiązania do poddania się leczeniu odwykowemu, oraz że znane mi są przepisy o odpowiedzialności karnej za udostępnienie danych osobowych lub umożliwienie do nich dostępu osobom nieuprawnionym.

.....  
(czytelny podpis )

Załącznik 3 do Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”

Czerwieńsk, dnia ..... r.

Nr ewidencyjny:.....

**UPOWAŻNIENIE**  
**do przetwarzania danych osobowych i danych wrażliwych**

1. Upoważniam **Panią/ Pana** ....., ..... GKRPA  
(Imię i nazwisko) (funkcja w Komisji)

do dostępu do następujących danych osobowych:

- dotyczących zgłaszanych osób nadużywających alkoholu i innych środków odurzających,
- dotyczących danych osobowych i miejsca zamieszkania osoby uzależnionej i jej rodziny,
- dotyczących niezbędnych informacji uzyskiwanych od instytucji (Sąd, Prokuratura, Policja, Kuratorzy, OPS, Placówki terapeutyczne, Szpitale itp.)
- dotyczących danych o stanie zdrowia i nałogach,
- dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym,
- podejmowanie czynności zmierzające do orzeczenia przez właściwy miejscowy sąd o zastosowaniu wobec osoby uzależnionej obowiązku poddania się leczeniu w zakładzie leczenia odwykowego dołączając zebrana dokumentację wraz z opinią biegłego.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej ( ewidencje, teczki osobowe, rejestry, spisy itp.) wg. wykazu zbiorów podanych w pkt. 2

Upoważnienie wydaje się na czas wykonywania funkcji w GKRPA i zobowiązania do zachowania tajemnicy, również po ustaniu pełnienia funkcji, oraz zachowania w tajemnicy informacji zabezpieczenia tych danych przed zniszczeniem i nielegalnym ujawnieniem.

2. Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach:

- a) teczki osobowe z zawartością wszystkich dokumentów otrzymanych i wytworzonych, prowadząc postępowanie wobec zgłoszonej osoby nadużywającej alkoholu i innych środków odurzających.
- b) Rejestr pism przychodzących oraz wychodzących i wytworzonych w formie papierowej.

Przyjmuję do wiadomości i stosowania:

Burmistrz Czerwieńska

.....  
(data i podpis)

.....  
(podpis)

Niniejsze upoważnienie zostało sporządzone w 3 egz.

1. Osoba upoważniona
2. Akta osobowe upoważnionego
3. Administrator Ochrony Danych



Załącznik 4 do Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”

Czerwieńsk, dnia ..... r.

.....  
(imię i nazwisko )

.....  
(stanowisko w GKRP)

.....

.....  
(adres zamieszkania)

**OŚWIADCZENIE**  
**O ZAPOZNANIU SIĘ Z TREŚCIĄ REGULAMINU GMINNEJ KOMISJI**  
**ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH W CZERWIEŃSKU**

Niniejszym potwierdzam, że zapoznałem/am się z treścią regulaminu Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku.

.....  
(czytelny podpis )

Załącznik 5 do Polityki Bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Czerwieńsku”

## **INSTRUKCJA**

### **postępowania w sytuacji naruszenia ochrony danych osobowych**

#### **I. Istota naruszenia danych osobowych**

§ 1.

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego,

a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

#### **II. Postępowanie w przypadku naruszenia danych osobowych**

§ 2.

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:
  - a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
  - b. dokumentacja jest niszczone bez użycia niszczarki;
  - c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
  - d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
  - e. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
  - f. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
  - g. wnoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
  - h. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
  - i. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
  - j. telefoniczne próby wyłudzenia danych osobowych;
  - k. kradzież komputerów lub twardych dysków z danymi osobowymi;
  - l. utrata kontroli nad kopią danych osobowych;

- m. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
- n. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
- o. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"
- p. hasła do systemów przechowywane są w pobliżu komputera.

§ 3.

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4.

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5.

Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6.

Inspektor ochrony danych podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
- odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7.

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport.

§ 8.

Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych)

### **III. Naruszenie danych osobowych - odpowiedzialność**

§ 9.

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza

odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę  
o zrekompensowanie poniesionych strat.

#### **IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu**

##### § 10.

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
  - a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
  - d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu weryfikowanie przestrzegania niniejszego artykułu.

#### **V. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych**

##### § 11.

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
  - a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku.

W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.



