



**POLITYKA BEZPIECZEŃSTWA OCHRONY  
DANYCH OSOBOWYCH  
W  
URZĘDZIE GMINY DOBRÓŃ  
UL. 11 Listopada 9 Dobroń**

## PODSTAWA PRAWNA

1. Konstytucja RP (art. 47 i 51).
2. Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych.
3. Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.
4. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2018 r. poz. 1000).

## PODSTAWOWE POJĘCIA

### § 1

1. UGD– w tym dokumencie jest rozumiana jako Urząd Gminy Dobroń
2. Polityka – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa” obowiązująca w UG w Dobroniu
3. Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora Danych Osobowych (Wójta Gminy Dobroń) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w SPS. IOD powołany jest Zarządzeniem Wójta Gminy Dobroń
4. Użytkownik – osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej, odbywająca staż.
5. Przetwarzanie danych – rozumie się to w tym dokumencie jako jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
6. Zabezpieczenie danych – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

## 2.

### POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

#### I.1. Wykaz budynków, w których przetwarzane są dane osobowe

### § 2

ADRES – BUDYNEK	POMIESZCZENIA
Dobroń ul. 11 listopada 9	Urząd Gminy - pomieszczenia biurowe

#### I.2 System przetwarzania danych osobowych

### § 3

W skład systemu wchodzi:

- 1) dokumentacja papierowa

- 2) wydruki komputerowe;
- 3) procedury przetwarzania danych, w tym procedury awaryjne.

### **I.2.1 Cele i zasady funkcjonowania polityki bezpieczeństwa**

#### **§ 4**

Realizując Politykę bezpieczeństwa informacji zapewnia ich:

- 1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
- 2) integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
- 3) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
- 4) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
- 5) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
- 6) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
- 7) niezawodność – zamierzone zachowania i skutki są spójne.

#### **§ 5**

Polityka ochrony danych osobowych w UG w Dobroniu ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, to jest:

- 1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone UGD;
- 2) naruszeń przepisów prawa oraz innych regulacji;
- 3) utraty lub obniżenia reputacji;
- 4) strat finansowych ponoszonych w wyniku nałożonych kar.

#### **§ 6**

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych AD (Administrator Danych) dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

- 1) przetwarzane zgodnie z prawem,
- 2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- 3) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
- 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

### **I.2.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych**

#### **§ 7**

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy lub kodeksie cywilnym

#### **§ 8**

Administrator Danych Osobowych (ADO) – Wójt Gminy Dobroń:

- 1) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- 2) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- 3) odpowiada za zgodne z prawem przetwarzanie danych osobowych w UGD.

#### **§ 9**

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Wójta Gminy w Dobroniu:

- 1) egzekwuje zgodnie z prawem przetwarzanie danych osobowych w UGD w imieniu ADO; wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa załącznik nr 1;
- 2) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa załącznik nr 2;
- 3) ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa załącznik nr 3;
- 4) prowadzi rejestr zbiorów danych osobowych, według wzoru określonego w załączniku nr 7;
- 5) określa potrzeby w zakresie stosowanych w UGD zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia;
- 6) udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa;
- 7) bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w UGD i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

### **I.2.3 Zasady udzielania dostępu do danych osobowych**

#### **§ 10**

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w UGD polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.

#### **§ 11**

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez IOD.

#### **§ 12**

IOD może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników UGD do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w UGD.

### **I.2.4 Udostępnianie i powierzanie danych osobowych**

#### **§ 13**

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

#### **§ 14**

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

- 1) adresat wniosku (administrator danych),
- 2) wnioskodawca,
- 3) podstawa prawna (wskazanie potrzeby),
- 4) wskazanie przeznaczenia,
- 5) zakres informacji.

#### **§ 15**

Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

#### **§ 16**

Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

#### **§ 17**

Każda osoba fizyczna, której dane przetwarzane są w UGD, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art.32ust 1pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

#### **§ 18**

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi IOD, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w załączniku nr 4.

### **I.2.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej**

#### **§ 19**

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone zamknięciem zbioru danych w szafie na klucz. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

## § 20

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

## § 21

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w UGD powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z IOD w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

### I.3 Analiza ryzyka związanego z przetwarzaniem danych osobowych

#### I.3.1 Identyfikacja zagrożeń

## § 22

<b>FORMA PRZETWARZANIA DANYCH</b>	<b>ZAGROŻENIA</b>
<b>dane przetwarzane w sposób tradycyjny</b>	<ul style="list-style-type: none"><li>- oszustwo, kradzież, sabotaż;</li><li>- zdarzenia losowe (pożar);</li><li>- zaniedbania pracowników UGD (niedyskrecja, udostępnienie danych osobie nieupoważnionej);</li><li>- niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;</li><li>- pokonanie zabezpieczeń fizycznych;</li><li>- podsłuchy, podglądy;</li><li>- ataki terrorystyczne;</li><li>- brak rejestrowania udostępniania danych;</li><li>- niewłaściwe miejsce i sposób przechowywania. dokumentacji;</li></ul>
<b>dane przetwarzane w systemach informatycznych</b>	<ul style="list-style-type: none"><li>- oszustwo, kradzież, sabotaż;</li><li>- zaniedbania pracowników UGD (niedyskrecja, udostępnienie danych osobie nieupoważnionej);</li><li>- niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;</li><li>- pokonanie zabezpieczeń informatycznych;</li><li>- podsłuchy, podglądy;</li><li>- ataki terrorystyczne;</li><li>- pozostawienie sprzętu bez wylogowania się.</li></ul>

#### I.6.2 Sposób zabezpieczenia danych

## § 23

<b>FORMA PRZETWARZANIA DANYCH</b>	<b>STOSOWANE ŚRODKI OCHRONY</b>
<b>dane przetwarzane w systemach informatycznych</b>	<ul style="list-style-type: none"><li>- przetwarzanie danych osobowych tylko w komputerach specjalnie do tego przystosowanych,</li><li>- zastosowanie haseł w dostępie do komputera;</li><li>- przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez IOD;</li><li>- zapoznanie pracowników z zasadami przetwarzania danych</li></ul>

	osobowych oraz obsługą - monitoring wizyjny
<b>dane przetwarzane w sposób tradycyjny</b>	- przechowywanie danych w pomieszczeniach zamykanych na zamki, - przechowywanie danych osobowych w szafach zamykanych na klucz, - osoby z ochrony wydające klucze tylko osobom upoważnionym, - przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez IOD, - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania, - monitoring wizyjny

### **I.3.3 Określenie wielkości ryzyka**

#### **§ 24**

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

### **I.3.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń**

#### **§ 25**

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. IOD przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

## **INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH**

### **II.1 Istota naruszenia danych osobowych**

#### **§ 26**

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

- 1) nieautoryzowany dostęp do danych;
- 2) nieautoryzowane modyfikacje lub zniszczenie danych;
- 3) udostępnienie danych nieautoryzowanym podmiotom;
- 4) nielegalne ujawnienie danych;
- 5) pozyskiwanie danych z nielegalnych źródeł.

### **II.2 Postępowanie w przypadku naruszenia danych osobowych**

#### **§ 27**

Każdy pracownik oraz osoba pracująca na podstawie umowy cywilnej lub cywilno-prawnej w UGD, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to IOD.

#### **§ 28**

Każdy pracownik oraz osoba pracująca na podstawie umowy cywilnej lub cywilno-prawnej w UGD, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

#### **§ 29**

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 IOD.

#### **§ 30**

IOD podejmuje następujące kroki:

- 1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy UGD;
- 2) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
- 3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu ADO, nawiązuje kontakt ze specjalistami poza urzędem (jeśli zachodzi taka potrzeba).

#### **§ 31**

IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik nr 5 i przekazuje go ADO.

#### **§ 32**

IOD 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).

### **II.3 Sankcje karne**

#### **§ 33**

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczynają się postępowanie dyscyplinarne.

#### **§ 34**

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.