

## Spis treści

1. Podstawa i cel Polityki.....	2
2. Definicje i terminy użyte w Polityce.....	3
3. Administrator Danych Osobowych – obowiązki i odpowiedzialność.....	4
4. Personel ADO.....	6
5. Powierzenie przetwarzania danych osobowych.....	6
6. Zasady udostępniania danych osobowych.....	7
7. Zbiory danych osobowych przetwarzane przez DGCS.NET.....	7
8. Środki ochrony fizycznej.....	7
9. Środki sprzętowe, informatyczne i telekomunikacyjne.....	8
10. Środki organizacyjne.....	9
Załącznik nr 1.....	10
Załącznik nr 2.....	11
Załącznik nr 3.....	12
Załącznik nr 4.....	13
Załącznik nr 5.....	14

---

---

## Podstawa i cel Polityki

1.1. Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024).

1.2. Polityka bezpieczeństwa obejmuje swoim zakresem zbiory danych osobowych, które przetwarzane są przez Przedsiębiorstwo DGCS.NET, zwany w dalszej części Polityki DGCS.NET Sp. z o. o.)

1.3. Podstawy prawne w zakresie Polityki bezpieczeństwa danych osobowych stanowią:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2002 r. Nr 101 poz. 926 z późniejszymi zmianami),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100 poz. 1024),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536).

1.4. Zasady określone przez dokument Polityka bezpieczeństwa mają zastosowanie do:

- Danych osobowych przetwarzanych przez DGCS.NET, zarówno w przypadku, gdy jest on administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone jemu na podstawie umów zawartych w trybie art. 31 ustawy o ochronie danych osobowych,
- Wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie,
- Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie,
- Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do danych osobowych podlegających ochronie.

- 1.5. Celem niniejszej Polityki bezpieczeństwa jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczać dane osobowe, a zatem organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych oraz edukowanie użytkowników systemu ochrony danych osobowych.
- 1.6. Polityka bezpieczeństwa dotyczy zadań związanych z zabezpieczeniem danych osobowych zarówno przetwarzanych w sposób tradycyjny (papierowy) jak i w systemach informatycznych. Wszyscy pracownicy DGCS.NET zobowiązani są do przestrzegania postanowień Polityki.
- 1.7. Naruszanie Ustawy o ochronie danych osobowych zagrożone jest konsekwencjami karnymi określonymi w jej zapisach.

## 2. Definicje i terminy użyte w Polityce

- 2.1. **Administrator Danych Osobowych (zwany dalej ADO)** – DGCS.NET, decyduje o celach i środkach przetwarzania danych osobowych, jego przedstawicielem jest Prezes Zarządu.
- 2.2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez administratora danych zarówno w systemach informatycznych jak i tradycyjnie (wersja papierowa).
- 2.3. **GIODO** - Generalny Inspektor Ochrony Danych Osobowych.
- 2.4. **Nośniki danych** – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne.
- 2.5. **Odbiorca danych** - każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela podmiotu przetwarzającego dane osobowe mający siedzibę lub miejsce zamieszkania w państwie trzecim, podmiotu, któremu powierzono przetwarzanie danych osobowych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
- 2.6. **Personel** – wszystkie osoby mające dostęp do danych osobowych u ADO.
- 2.7. **Przetwarzanie danych osobowych** – jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, w szczególności w systemach informatycznych.

2.8. **System informatyczny** – zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe.

2.9. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

### 3. Administrator Danych Osobowych – obowiązki i odpowiedzialność

Do podstawowych obowiązków ADO należy:

3.1. **Zapewnienie** środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:

- Udostępnieniem osobom nieupoważnionym,
- Zabranieniem przez osobę nieuprawnioną,
- Zmianą, utratą, uszkodzeniem lub zniszczeniem.

3.2. Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

- Została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych,
- Został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą,
- Dane były przetwarzane zgodnie z obowiązującymi przepisami prawa oraz normami i dobrymi praktykami oraz normami społecznymi,
- Dane zbierane były w oznaczonym zgodnym z prawem celem,
- Dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania,
- Były przetwarzane z ograniczeniem czasowym.

3.3. Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności:

- Polityki bezpieczeństwa danych osobowych,
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

3.4. Wyznaczenie ABI nadzorującego przestrzeganie zasad ochrony w przypadku, w którym ADO nie wykonuje tych obowiązków sam.

3.5. Dopuszczanie do przetwarzania danych wyłącznie osoby posiadającej imienne upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.

- 3.6. Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).
- 3.7. Respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:
  - ADO,
  - Celu, zakresie i sposobie przetwarzania danych,
  - Terminu od kiedy i jakie dane są przetwarzane,
  - Źródle, z którego dane pochodzą,
  - Sposobie udostępniania danych oraz ich odbiorcach.
- 3.8. Respektowanie praw osób, których dane dotyczą w zakresie:
  - Żądania uzupełnienia, uaktualnienia, sprostowania danych,
  - Wniesienia umotywowanego wniosku do zaprzestania przetwarzania danych.
- 3.9. Sporządzanie i wprowadzenie w życie zasad bezpiecznego przetwarzania danych osobowych, w szczególności w systemach informatycznych.
- 3.10. Opracowanie i aktualizację „Polityki bezpieczeństwa”.
- 3.11. Opracowanie „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych” i czuwanie nad jej przestrzeganiem.
- 3.12. Prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych.
- 3.13. Nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe.
- 3.14. Uczestniczenie w czynnościach kontrolnych GIODO.
- 3.15. Nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe, w tym nadzorowanie dostępu do tych pomieszczeń oraz kontrolę przebywających w nich osób.
- 3.16. Wykonywanie rejestracji i aktualizacji zbiorów danych w rejestrze prowadzonym przez GIODO.
- 3.17. Zapewnienie prawidłowej eksploatacji systemu informatycznego, zgodnej z celami przetwarzania danych osobowych.
- 3.18. Nadzorowanie wykonywania kopii zapasowych, odpowiedniego ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu.
- 3.19. Zapewnienie ochrony nośników zawierających kopie zbiorów danych osobowych.

## Personel ADO

- 4.1. Pracownicy ADO zobowiązani są do zapoznania się z treścią dokumentacji określającą sposób postępowania przy przetwarzaniu danych osobowych.
- 4.2. Każdy pracownik podpisuje oświadczenie zawierające deklarację znajomości i stosowania wymogów określonej w pkt. 6.1. dokumentacji (Załącznik nr 2 Polityki).
- 4.3. Oświadczenia, o których mowa powyżej przechowywane są w aktach osobowych pracownika.

## 5. Powierzenie przetwarzania danych osobowych

- 5.1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi na podstawie umowy powierzenia zawartej na piśmie.
- 5.2. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO.
- 5.3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.
- 5.4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:
  - Stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane oraz tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe,
  - Opracowania dokumentacji dotyczącej przetwarzania danych osobowych,
  - Niezwłocznego powiadomienia ADO o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia,
  - Zapewnienia, aby każda osoba stanowiąca personel podmiotu zewnętrznego przetwarzająca powierzone dane osobowe posiadała upoważnienie do przetwarzania tych danych osobowych,
  - Zniszczenia lub zwrotu przekazanych danych stosownie do zapisów umowy powierzenia przetwarzania danych.

## Zasady udostępniania danych osobowych

6.1. Udostępnianie danych jest jedną z form ich przetwarzania.

6.2. Udostępnianie danych osobowych odbiorcom danych może nastąpić, podobnie jak przetwarzanie danych, w przypadku spełnienia jednej z przesłanek określonych w art. 23 ust. 1 pkt 1-5 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tj:

- Osoba, której dane dotyczą, wyrazi na to zgodę,
- Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

6.3. Osoby upoważnione do przetwarzania danych, którzy w ramach swych obowiązków służbowych udostępniają dane osobowe mają obowiązek prowadzić ewidencję danych, które są udostępniane (określającą odbiorcę danych, przyczynę udostępnienia, zakres danych oraz datę udostępnienia).

6.4. Wzór ewidencji określonej w p. 8.3 stanowi Załącznik nr 5 Polityki.

## 7. Zbiory danych osobowych przetwarzane przez DGCS.NET

Kompletna lista zbiorów danych osobowych przetwarzanych przez DGCS.NET została określona w Załączniku nr 1 Polityki.

## 8. Środki ochrony fizycznej

8.1. Pomieszczenia biurowe ADO, w których przetwarzane są dane osobowe winne być zabezpieczone od zewnątrz drzwiami zwykłymi bądź wzmocnionymi zamykanymi na klucz.

8.2. Osoby nieupoważnione mogą przebywać w pomieszczeniach wyłącznie w obecności osób upoważnionych z ramienia ADO i tylko w czasie wymaganym na wykonanie niezbędnych czynności

8.3. Dokumenty papierowe zawierające dane osobowe winny być przechowywane są w szafach zamykanych na klucz.

8.4. Po ustaniu przydatności dokumentacja papierowa zawierająca dane osobowe powinna być niszczone mechanicznie z użyciem niszczarki dokumentów.

## 9. Środki sprzętowe, informatyczne i telekomunikacyjne

9.1. Dane osobowe przetwarzane przy użyciu systemu informatycznego są zabezpieczone przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla oraz programu antywirusowego.

9.2. Oprogramowanie antywirusowe oraz firewall wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie.

9.3. Wszelkie systemy informatyczne ADO służące do przetwarzania danych osobowych mogą być wykorzystane wyłącznie w celach służbowych.

9.4. Zasoby systemu informatycznego przetwarzane mogą być wyłącznie zgodnie z ich przeznaczeniem.

9.5. Dostęp do systemu operacyjnego komputera oraz aplikacji, w których są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem indywidualnego identyfikatora użytkownika oraz hasła.

9.6. W związku z zastosowaniem przez ADO środków bezpieczeństwa na poziomie wysokim (określonych w p. 1 Załącznika do Rozporządzenia), hasło zabezpieczające musi się składać z minimum 8 znaków, zawierających małe i wielkie litery, cyfry lub znaki specjalne.

9.7. W związku z zastosowaniem środków bezpieczeństwa na poziomie wysokim hasło musi być zmieniane cyklicznie, nie rzadziej niż raz na 30 dni.

## 10. Środki organizacyjne

10.1. ADO przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia ADO określającego zakres uprawnień pracownika według wzoru określonego w Załączniku Nr 3 Polityki.

10.2. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem ich do pracy z tymi danymi powinny zostać zaznajomione w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych.



10.3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych w DGCS.NET według wzoru określonego w załączniku Nr 4.

**Załącznik nr 1****Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez DGCS.NET****Rejestr zbiorów danych osobowych przetwarzanych przez DGCS.NET**

L P	Nazwa zbioru	Zakres przetwarzanych danych osobowych	Zgłoszenie do GIODO
1	Zbiór danych osobowych pracowników stanowiących personel ADO a także wykonujących na jego rzecz czynności związane ze świadczeniem pracy.	<ul style="list-style-type: none"> <li>• Imiona i nazwisko,</li> <li>• Imiona rodziców,</li> <li>• Data i miejsce urodzenia,</li> <li>• Adres zamieszkania,</li> <li>• PESEL,</li> <li>• NIP,</li> <li>• Seria i numer dowodu osobistego,</li> <li>• Zawód wyuczony oraz wykonywany,</li> <li>• Obywatelstwo,</li> <li>• Przebieg pracy zawodowej,</li> <li>• Informacje dotyczące wykształcenia,</li> <li>• Imiona i nazwiska, daty urodzenia dzieci,</li> <li>• Numer rachunku bankowego.</li> </ul>	Nie podlega zgłoszeniu zgodnie z art. 43 Ustawy.
2	Zbiór danych osobowych klientów oraz potencjalnych klientów sklepu internetowego przetwarzany w celu świadczenia usługi sprzedaży i/lub powiadamiania o akcjach marketingowych i promocjach (newsletter)	<ul style="list-style-type: none"> <li>• Imię i nazwisko,</li> <li>• Adres zamieszkania/dostawy,</li> <li>• Adres e-mail,</li> <li>• Numer NIP,</li> <li>• Nr telefonu.</li> </ul>	Podlegający zgłoszeniu zgodnie z art. 40 Ustawy.
3	Zbiór danych osobowych klientów salonów sprzedaży	<ul style="list-style-type: none"> <li>• Imię i nazwisko,</li> <li>• Adres zamieszkania/dostawy,</li> <li>• Adres e-mail,</li> <li>• Nr telefonu.</li> </ul>	Nie podlega zgłoszeniu zgodnie z art. 43 Ustawy.
4	Zbiór danych osobowych zawarte na protokołach reklamacyjnych	<ul style="list-style-type: none"> <li>• Imię i nazwisko,</li> <li>• Adres zamieszkania/dostawy,</li> <li>• Adres e-mail,</li> <li>• Nr telefonu.</li> </ul>	Podlegający zgłoszeniu zgodnie z art. 40 Ustawy.

**Załącznik nr 2**

(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez DGCS.NET

.....  
(nazwisko i imię)

.....  
(stanowisko)

**OŚWIADCZENIE**

Ja, niżej podpisany oświadczam, iż w związku z pracą przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, a także z wdrożoną w DGCS.NET dokumentacją związaną z ochroną danych osobowych.

.....  
(podpis oświadczającego)

**Załącznik nr 3**

(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez DGCS.NET

**UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH**

Na podstawie Art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.), **upoważniam**

Pana/Panią

.....  
( imię nazwisko)

.....  
( stanowisko służbowe)

Do przetwarzania danych osobowych w następującym zakresie:

1. Zbieranie.
2. Utrwalanie.
3. Przechowywanie.
4. Opracowanie.
5. Zmianianie.
6. Usuwanie.

Niniejsze upoważnienie jest ważne do odwołania.

.....  
(data i podpis w imieniu Administratora Danych Osobowych)

**Załącznik nr 4**

(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez DGCS.NET**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**

Nazwisko i imię	Stanowisko służbowe	Zakres upoważnienia do przetwarzania danych osobowych	Nr upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator (jeśli dane przetwarzane są w systemie informatycznym)

**Załącznik nr 5**

(wzór)

Do Polityki bezpieczeństwa danych osobowych przetwarzanych przez DGCS.NET

**EWIDENCJA UDOSTĘPNIANIA DANYCH OSOBOWYCH**

LP	Odbiorca danych osobowych (nazwa)	Przyczyna udostępnienia danych osobowych	Zakres udostępnionych danych	Data udostępnienia