Warszawa, dnia 17-11-2022 r.

Poz. 15

# Z A R Z Ą D Z E N I E  N R  1 4

# G E N E R A L N E G O  D Y R E K T O R A

# O C H R O N Y  Ś R O D O W I S K A

z dnia 17 listopada 2022 r.

**w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska**

Na podstawie § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) zarządza się, co następuje:

**§ 1.** W Generalnej Dyrekcji Ochrony Środowiska ustanawia i wdraża się System Zarządzania Bezpieczeństwem Informacji, który obejmuje dokumentację Systemu Zarządzania Bezpieczeństwa Informacji, a także strukturę organizacyjną, planowane działania i zasoby.

**§ 2.** Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji obejmuje:

1) Politykę Bezpieczeństwa Informacji Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 1 do niniejszego Zarządzenia;
2) Politykę przetwarzania danych osobowych w Generalnej Dyrekcji Ochrony Środowiska stanowiącą załącznik nr 2 do niniejszego Zarządzenia;
3) Regulamin Bezpieczeństwa Informacji Generalnej Dyrekcji Ochrony Środowiska – stanowiący załącznik nr 3 do niniejszego Zarządzenia;

4) Procedurę nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 4 do niniejszego Zarządzenia;
5) Procedurę zarządzania incydentami bezpieczeństwa informacji, w tym danych osobowych w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 5 do niniejszego Zarządzenia;
6) Procedurę zarządzania ryzykiem wraz z metodyką szacowania ryzyka w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 6 do niniejszego Zarządzenia;
7) Politykę Bezpieczeństwa Teleinformatycznego Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 1 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
8) Procedurę kontroli dostępu do aktywów informacyjnych w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 2 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
9) Procedurę niszczenia nośników oraz przekazywania do ponownego użycia w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 3 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
10) Procedurę pomiaru i oceny skuteczności zabezpieczeń w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 4 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
11) Procedurę wykonywania kopii zapasowych w Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 5 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
12) Procedurę zarządzania konfiguracją i zmianami systemu teleinformatycznego Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 6 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
13) Procedurę zarządzania ciągłością działania systemu teleinformatycznego Generalnej Dyrekcji Ochrony Środowiska – stanowiącą załącznik nr 7 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
14) Procedurę zarządzania poprawkami – stanowiącą załącznik nr 8 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;

15) Zasady bezpieczeństwa fizycznego w Generalnej Dyrekcji Ochrony Środowiska – stanowiące załącznik nr 9 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.;
16) Zasady bezpieczeństwa w relacjach z dostawcami w Generalnej Dyrekcji Ochrony Środowiska – stanowiące załącznik nr 10 do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r.

**§ 3.** Tracą moc:

1) zarządzenie nr 12 Generalnego Dyrektora Ochrony Środowiska z dnia 17 grudnia 2015 r. w sprawie sposobu rejestracji zbiorów danych osobowych w Generalnej Dyrekcji Ochrony Środowiska;
2) zarządzenie nr 7 Generalnego Dyrektora Ochrony Środowiska z dnia 14 marca 2019 r. w sprawie Polityki przetwarzania danych osobowych w generalnej Dyrekcji Ochrony Środowiska;
3) zarządzenie nr 8 Generalnego Dyrektora Ochrony Środowiska z dnia 14 marca 2019 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska.

**§ 4.** Zarządzenie wchodzi w życie z dniem 1 grudnia 2022 r.

**GENERALNY DYREKTOR**
**OCHRONY ŚRODOWISKA**

ANDRZEJ SZWEDA-LEWANDOWSKI
Generalny Dyrektor Ochrony Środowiska
Generalny Dyrektor Ochrony Środowiska
/ – podpisany cyfrowo/

**Załącznik nr 1** do Zarządzenia nr 14 Generalnego Dyrektora Ochrony Środowiska w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska z dnia 17 listopada 2022 r.

# *Polityka Bezpieczeństwa Informacji*
# Generalnej Dyrekcji Ochrony Środowiska

ZATWIERDZAM

Generalny Dyrektor Ochrony Środowiska

ANDRZEJ SZWEDA-LEWANDOWSKI

Generalny Dyrektor Ochrony Środowiska

.....

Generalny Dyrektor Ochrony Środowiska

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

1. Niniejsza Polityka Bezpieczeństwa Informacji, zwana dalej „PBI", określa cele i zakres Systemu Zarządzania Bezpieczeństwem Informacji, zwanym dalej „SZBI", jak również sposób postępowania i cele Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ", w odniesieniu do bezpieczeństwa informacji, tym samym zapewniając ramy dla wszelkich działań, uwzględniając zapewnienie poufności, integralności oraz dostępności informacji.
2. Niniejsza PBI stanowi podstawowy dokument SZBI.

## § 2. Zakres SZBI

1. SZBI oraz związane z nim procedury i obowiązujące zasady wynikające z wdrożonych dokumentów mają zastosowanie do wszystkich realizowanych procesów i zadań oraz lokalizacji GDOŚ.
2. Procesy objęte SZBI:
   1) Procesy realizowane przez Biuro Dyrektora Generalnego:
      a) Proces finansowy realizowany przez Zespół do spraw Budżetu i Finansów – właściciel procesu: Główny Księgowy,
      b) Proces kadrowy – właściciel procesu: Naczelnik Wydziału Kadr,
      c) Proces organizacyjny – właściciel procesu: Naczelnik Wydziału Organizacyjnego,
      d) Proces gospodarowania mieniem – właściciel procesu: Naczelnik Wydziału Organizacyjnego,
      e) Proces informatyczny - właściciel procesu: Naczelnik Wydziału Informatyki,
      f) Proces kontroli zarządczej - właściciel procesu: Dyrektor Biura;
   2) Proces prawny realizowany przez Biuro Prawne, w tym obsługa prawna Generalnego Dyrektora Ochrony Środowiska, wydawanie opinii prawnych na potrzeby działalności urzędu, przygotowywanie projektów aktów normatywnych pod względem legislacyjno-prawnym, obsługa zamówień publicznych, skarg i wniosków oraz realizacja zadań dotyczących systemu ekozarządzania i audytu (EMAS) – właściciel procesu: Dyrektor Biura;
   3) Proces obsługi projektów realizowanych przez Departament Realizacji Projektów Środowiskowych, w tym przygotowywanie wniosków o dofinansowanie i realizacja projektów dofinansowywanych ze środków Programu LIFE, Programu Operacyjnego Infrastruktura i Środowisko (POIiŚ) oraz Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej, inicjowanie i realizacja projektów dofinansowywanych z innych źródeł, obsługa projektów związanych z wynagrodzeniami i podnoszeniem kwalifikacji oraz koordynacja ich wdrażania w regionalnych dyrekcjach ochrony środowiska – właściciel procesu: Dyrektor Departamentu;
   4) Proces oceny oddziaływania na środowisko realizowany przez Departament Ocen Oddziaływania na Środowisko – właściciel procesu: Dyrektor Departamentu;
   5) Proces prowadzenia postępowań administracyjnych realizowany przez Departament Orzecznictwa Administracyjnego – właściciel procesu: Dyrektor Departamentu;
   6) Proces wydawania zezwoleń realizowany przez Departament Zarządzania Zasobami Przyrody, w tym wydawanie zezwoleń z zakresu szeroko pojętej ochrony gatunkowej i odstępstw od zakazów w rezerwatach, koordynacja sieci Natura 2000 w Polsce, prowadzenie baz danych (m.in. baza Natura 2000, Centralny Rejestr Ochrony Przyrody), opracowywanie aktów prawnych dla obszarów Natura

2000 (ustanawianie obszarów), opiniowanie dokumentów planistycznych dla obszarów Natura 2000 – właściciel procesu - Dyrektor Departamentu.

3. SZBI obejmuje całą strukturę organizacyjną GDOŚ.

4. SZBI obejmuje wszystkie lokalizacje, w których realizowane są procesy i zadania GDOŚ.

5. SZBI obejmuje cały System teleinformatyczny GDOŚ, w tym całą infrastrukturę sieciową i serwerową oraz systemy i aplikacje wykorzystywane w GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Polityce jest mowa o:

1) **Administratorze Bezpieczeństwa Fizycznego (ABF)** - należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze ochrony fizycznej Stref bezpieczeństwa w GDOŚ oraz odpowiada za zapewnienie bezpieczeństwa w tych strefach.

2) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez Administratora Danych Osobowych do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.

3) **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem Danych Osobowych jest Generalny Dyrektor Ochrony Środowiska, w imieniu którego zadania realizuje Dyrektor Generalny GDOŚ. W zakresie przetwarzania danych osobowych osób zatrudnionych w GDOŚ Administratorem Danych Osobowych jest Generalna Dyrekcja Ochrony Środowiska w imieniu której funkcję ADO wykonuje Dyrektor Generalny GDOŚ.

4) **Administratorze Merytorycznym Systemu (AMS)** – należy przez to rozumieć osobę wyznaczoną przez ABT i powołaną przez Dyrektora Generalnego GDOŚ do realizacji zadań związanych z obsługą danego systemu teleinformatycznego GDOŚ.

5) **Administratorze Technicznym Systemu (ATS)** – należy przez to rozumieć pracownika Wydziału Informatyki w Biurze Dyrektora Generalnego GDOŚ.

6) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną.

7) **BIA (Business Impact Analysis)** – należy przez to rozumieć analizę wpływu zakłóceń ciągłości działania systemów teleinformatycznych na funkcjonowanie GDOŚ.

8) **Ciągłości działania** – należy przez to rozumieć przeciwdziałanie przerwom w działalności GDOŚ oraz ochronę krytycznych procesów przetwarzania aktywów informacyjnych przed rozległymi awariami systemów informacyjnych lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie. Ogół działań wykonywanych przed, w trakcie i po awarii lub katastrofie w celu utrzymania realizacji zadań GDOŚ.

9) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres

zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

10) **DRP** – należy przez to rozumieć Plany Odtworzenia po Katastrofie.

11) **Dyrektorze Departamentu lub Biura –** należy przez to rozumieć dyrektora departamentu albo biura, jego zastępcę lub inną osobę wyznaczoną do kierowania komórką organizacyjną.

12) **Incydencie** – należy przez to rozumieć pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań GDOŚ i zagrażają bezpieczeństwu informacji.

13) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 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), którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

14) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;

15) **ISCP** – należy przez to rozumieć Plany Awaryjne Systemów Informatycznych.

16) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.

17) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.).

18) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialności za bezpieczeństwo informacji i zarządzanie SZBI

1. W celu zagwarantowania bezpieczeństwa informacji oraz prawidłowego i zgodnego z przepisami ich przetwarzania, Dyrektor Generalny GDOŚ powołuje Zespół do spraw zarządzania bezpieczeństwem informacji, zwany dalej **„Zespołem ds. ZBI”**.
2. Do zadań Zespołu ds. ZBI należy monitorowanie i koordynowanie, wraz z Pełnomocnikiem ds. BI, działań związanych z bezpieczeństwem informacji.
3. Dyrektor Generalny GDOŚ wyznacza:
   1) Pełnomocnika ds. BI, któremu może powierzyć funkcję przewodniczącego Zespołu ds. ZBI
   2) ABT;

3) ATS;
4) AMS;
5) ABF.

4. W skład Zespołu ds. ZBI wchodzą:
   1) Pełnomocnik ds. BI;
   2) ABT;
   3) IOD;
   4) przedstawiciel ADO;
   5) ABF;
   6) Pełnomocnik ds. Ochrony Informacji Niejawnych;
   7) Dyrektorzy Departamentów lub Biur.
5. Dyrektor Generalny GDOŚ odpowiada za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia SZBI oraz wskazanych w nim odpowiednich zabezpieczeń, w tym zapewnienie niezbędnych zasobów do skutecznego zarządzania bezpieczeństwem teleinformatycznym, a w szczególności:
   1) wprowadza, zarządza przy pomocy Pełnomocnika ds. BI i sprawuje nadzór nad działaniem SZBI;
   2) określa rodzaje zasobów podlegających ochronie;
   3) decyduje o celach i środkach przetwarzania danych;
6. Pełnomocnik ds. BI:
   1) sprawuje nadzór nad dokumentacją SZBI na etapie jej opracowywania, weryfikacji, aktualizacji, udostępniania, przechowywania i archiwizacji zgodnie z ***Procedurą nadzoru nad dokumentacją***;
   2) sprawuje nadzór nad realizacją Polityki Bezpieczeństwa Informacji oraz procedur ustanowionych w ramach SZBI, z zastrzeżeniem ust. 11 pkt 1;
   3) zapewnia, że procesy niezbędne do prawidłowego funkcjonowania SZBI są ustanowione, wdrożone i utrzymywane;
   4) sprawuje nadzór nad planowaniem prac dotyczących SZBI oraz ich realizacją;
   5) nadzoruje opracowanie Strategii Ciągłości Działania oraz monitoruje Ciągłość działania Systemów teleinformatycznych GDOŚ zgodnie z ***Procedurą zarządzania ciągłością działania Systemu teleinformatycznego GDOŚ****;*
   6) nadzoruje proces zarządzania ryzykiem w bezpieczeństwie informacji w GDOŚ zgodnie z ***Procedurą zarządzania ryzykiem***
   7) koordynuje obsługę wszystkich zgłaszanych Incydentów zgodnie z ***Procedurą zgłaszania Incydentów***, w szczególności nadzoruje natychmiastowe reagowanie na zgłaszane Incydenty ustalanie przyczyn i skutków zgłaszanych Incydentów wraz z gromadzeniem materiału dowodowego, a także opracowanie i przedstawienie propozycji działań naprawczych oraz monitorowanie i dokumentowanie realizacji tych działań;
   8) uzyskuje wyjaśnienia od Pracowników w zakresie realizowanych działań w ramach SZBI;
   9) przedstawia sprawozdania do Dyrektora Generalnego GDOŚ dotyczące funkcjonowania SZBI oraz realizacji celów, jak również informuje o skuteczności funkcjonującego SZBI;

10) nadzoruje działania korygujące oraz doskonalące w ramach SZBI;
11) organizuje przeglądy SZBI oraz nadzoruje realizację ustaleń wynikających z przeglądów;
12) nadzoruje szkolenia z zakresu SZBI;
13) utrzymuje wykaz Aktywów informacyjnych;
14) analizuje raporty z wszelkich zdarzeń związanych z bezpieczeństwem informacji;
15) monitoruje poziom bezpieczeństwa informacji.

7. Pełnomocnik ds. BI uprawniony jest do:
   1) wydawania poleceń wszystkim pracownikom w zakresie związanym z wdrożeniem, utrzymaniem i doskonaleniem SZBI;
   2) analizy sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentacji SZBI oraz wydawania opinii w tym zakresie;
   3) dostępu do wszystkich dokumentów występujących w GDOŚ, których treść może być istotna z punktu widzenia funkcjonowania SZBI;
   4) uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach SZBI;
   5) reprezentowania GDOŚ na zewnątrz w sprawach dotyczących SZBI, bez możliwości zaciągania zobowiązań w imieniu GDOŚ.
8. ABT:
   1) odpowiada za bezpieczeństwo sieci teleinformatycznej;
   2) odpowiada za utrzymanie i stan okablowania sieci teleinformatycznej oraz okablowania zasilającego;
   3) odpowiada za utrzymywanie aktualnej dokumentacji sieci teleinformatycznej, dokumentacji dla Systemów teleinformatycznych w GDOŚ;
   4) koordynuje realizację zadań w zakresie zarządzania bezpieczeństwem teleinformatycznym w GDOŚ;
   5) monitoruje zgodność Systemów teleinformatycznych GDOŚ oraz aplikacji z Polityką Bezpieczeństwa Teleinformatycznego;
   6) zapewnia właściwą konfigurację i wydajność Systemów teleinformatycznych GDOŚ;
   7) administruje infrastrukturą i zasobami sieci w stopniu umożliwiającym zachowanie bezpieczeństwa sieci i zabezpieczenie danych przed nieupoważnionym dostępem;
   8) zapewnia Ciągłość działania i odpowiednią dostępność usług uruchomionych w ramach infrastruktury teleinformatycznej.
   9) sprawuje nadzór nad instalowaniem i konfigurowaniem sprzętów, systemów i aplikacji;
   10) odpowiada za współpracę z dostawcami aplikacji;
   11) nadzoruje wdrożone aplikacje;
   12) odpowiada za opracowanie standardów bezpieczeństwa dotyczących Systemów teleinformatycznych GDOŚ oraz procedur zarządzania Systemami teleinformatycznymi GDOŚ;
   13) bieżącą ocenę zagrożeń w zakresie bezpieczeństwa Systemów informatycznych GDOŚ;
   14) ustalanie przyczyn i skutków zgłaszanych Incydentów bezpieczeństwa związanych z funkcjonowaniem Systemu teleinformatycznego w GDOŚ wraz z gromadzeniem materiału dowodowego;

15) w ramach ***Procedury kontroli dostępu*** odpowiada za zarządzanie kontami użytkowników, w tym zakładanie i blokowanie kont; techniczne zarządzanie uprawnieniami użytkowników, w tym nadawanie i odbieranie uprawnień oraz zarządzanie profilami uprawnień dla grup użytkowników, powiązanymi z ich zakresem czynności na stanowisku pracy, a także wykonywanie wraz z AMS regularnych przeglądów uprawnień w administrowanych systemach teleinformatycznych;

16) w ramach ***Procedury zarządzania ciągłością działania Systemu teleinformatycznego GDOŚ*** odpowiada za opracowanie i aktualizacje BIA, DRP, ISCP, opracowanie i aktualizacje Harmonogramu testowania DRP i ISCP oraz testowanie DRP i ISCP zgodnie z przyjętym harmonogramem;

17) w ramach ***Procedury wykonywania kopii zapasowych*** odpowiada za:

a) opracowanie i aktualizowanie harmonogramu wykonywania kopii zapasowych;

b) nadzorowanie wykonania kopii zapasowych zgodnie z przyjętym harmonogramem;

c) wykonywanie kopii zapasowych zgodnie z przyjętym harmonogramem;

d) opracowanie i aktualizowanie harmonogramu testowania kopii zapasowych;

e) wykonywanie testów kopii zapasowych zgodnie z przyjętym harmonogramem;

f) w przypadku wykrycia zakłócenia funkcjonowania systemu kopii zapasowych – podjęcie działań naprawczych;

g) opracowywanie raportów z testów odtworzenia kopii zapasowych.

9. ATS w ramach właściwego mu obszaru wykonywania obowiązków służbowych i zleconych zadań:

1) administruje oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemów i zabezpieczenie danych przed nieupoważnionym dostępem;

2) zarządza funkcjonalnością systemu informatycznego;

3) utrzymuje właściwą konfigurację wydajności oraz ciągłości pracy systemu informatycznego;

4) prowadzi dzienniki systemowe;

5) zarządza kopiami zapasowymi danych aplikacji i systemów, w tym danych osobowych;

6) prowadzi rejestry incydentów w Systemach informatycznych w GDOŚ;

7) zarządza infrastrukturą i zasobami sieci;

8) zarządza kopiami zapasowymi urządzeń sieciowych;

9) odpowiada za wykonywanie i odtwarzanie kopii bezpieczeństwa;

10) instaluje i konfiguruje urządzenia aktywne i infrastruktury sieciowej;

11) utrzymuje właściwą konfigurację i wydajność sieci;

12) zapewnienia bezpieczeństwo zasobów Systemów teleinformatycznych w GDOŚ zgodnie z WBT;

13) monitoruje zasoby Systemów teleinformatycznych w GDOŚ;

14) monitoruje bezpieczeństwo usług zewnętrznych;

15) odpowiada za stosowanie zapisów ***Procedury zarządzania ciągłością działania Systemu teleinformatycznego GDOŚ;***

10. AMS w ramach właściwego mu obszaru wykonywania obowiązków służbowych i zleconych zadań:

1) zarządza uprawnieniami w Systemach teleinformatycznych w GDOS;

2) zarządza funkcjonalnością Systemów teleinformatycznych w GDOŚ;

3) prowadzi ewidencje nadanych uprawnień dostępu do Systemów teleinformatycznych w GDOŚ;
4) opiniuje standardy bezpieczeństwa dotyczące Systemów teleinformatycznych w GDOŚ;
5) opiniuje procedury zarządzania Systemami teleinformatycznymi w GDOŚ;
6) zarządza kontami użytkowników, w tym zakłada i blokuje konta;
7) zarządza od strony technicznej uprawnieniami użytkowników, w tym nadaje i odbiera uprawnienia;
8) wykonuje, wraz z KKO, regularne przeglądy uprawnień w administrowanych Systemach teleinformatycznych.

11. ABF odpowiada za:
    1) nadzór nad stosowaniem zasad określonych w ***Polityce bezpieczeństwa fizycznego w GDOŚ***,
    2) definiowanie i przegląd Stref bezpieczeństwa zgodnie z ***Polityką bezpieczeństwa fizycznego w GDOŚ***;
12. KKO odpowiadają za:
    1) nadzorowanie przestrzegania zasad ochrony informacji przez podległych im pracowników;
    2) identyfikowanie zagrożeń dla bezpieczeństwa informacji;
    3) określanie oraz realizację działań zapobiegających zagrożeniom;
    4) zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy;
    5) poprawność merytoryczną danych gromadzonych za pomocą systemów teleinformatycznych;
    6) bezpieczeństwo przetwarzanych danych osobowych;
    7) wnioskowanie o nadanie, zmianę lub odebranie uprawnień;
    8) wprowadzanie zabezpieczeń dla zasobów, nad którymi sprawują nadzór;
    9) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa;
    10) określenie zakresu uprawnień podległych pracowników;
    11) wnioskowanie o nadanie uprawnień do ABT i AMS;
    12) weryfikację uprawnień podległych pracowników;
    13) zapewnienie stosowania zasad wynikających z niniejszej procedury przez podległych Pracowników.
    14) współpracę z Pełnomocnikiem ds. BI w zakresie realizacji zadań dotyczących bezpieczeństwa informacji;
    15) opiniowanie ***Polityki Bezpieczeństwa Informacji*** i ***Polityki Przetwarzania Danych Osobowych***;
    16) opiniowanie i wnioskowanie o zmiany do ***Regulaminu Bezpieczeństwa Informacji***;
    17) nadzorowanie przestrzegania ***Regulaminu Bezpieczeństwa Informacji***;
    18) ocenę pracy systemów teleinformatycznych w celu identyfikacji wszelkich nieprawidłowości w pracy systemów.
13. Pracownicy GDOŚ ponoszą odpowiedzialność za bezpieczeństwo informacji zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi, w tym m. in.:
    1) stosować zasady opisane w dokumentacji SZBI oraz innych dokumentach wewnętrznych;

2) chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
3) chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
4) chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione;
5) utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w GDOŚ;
6) stosować się do szczegółowych zaleceń w zakresie bezpiecznej obsługi systemu informatycznego.

14. IOD odpowiada za nadzorowanie zgodności przetwarzania danych osobowych z przepisami prawa. Szczegółowy zakres obowiązków IOD określono w ***Polityce Przetwarzania Danych Osobowych***.
15. Każda osoba upoważniona do przetwarzania danych osobowych lub dostępu do informacji chronionych GDOŚ zobowiązana jest do złożenia ***Oświadczenia o zobowiązaniu do zachowania poufności***.

## § 5. Rodzaje przetwarzanych informacji

1. W GDOŚ informacje są chronione na podstawie przepisów prawa, zawartych umów, regulacji wewnętrznych oraz ich krytyczności dla GDOŚ. W oparciu o te wymagania dokonuje się podziału na właściwe klasy chronionych informacji. Najważniejsze grupy informacji objęte wymaganiami to:
   1) informacje wytworzone i pozyskiwane przez GDOŚ w trakcie realizacji zadań publicznych oraz zawartych umów;
   2) dane osobowe;
   3) informacje i dane finansowe;
   4) informacje niejawne, których ochrona realizowana jest zgodnie z odrębną dokumentacją wdrożoną w GDOŚ zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742, z późn.).
2. Ochrona danych osobowych w GDOŚ realizowana jest z uwzględnieniem przepisów:
   1) 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 z 04.05.2016, str. 1);
   2) ustawy z 10 maja 2018 o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
3. Ochrona danych osobowych prowadzona jest zgodnie z Polityką Przetwarzania Danych Osobowych.
4. Informacje finansowe w Generalnej Dyrekcji Ochrony Środowiska są chronione zgodnie z przepisami ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, z późn. zm.) oraz ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2021 r. poz. 305, z późn. zm.).

## § 6. Cele bezpieczeństwa informacji

1. Ogólne cele SZBI obejmują: bezpieczne przetwarzanie informacji w całym ich cyklu życia w celu spełnienia wymagań interesariuszy wewnętrznych i zewnętrznych oraz zmniejszanie szkód spowodowanych potencjalnymi incydentami. Dyrektor Generalny GDOŚ jest uprawniony do ustalania celów SZBI innych niż wskazane w zdaniu poprzednim.
2. Dyrektor Generalny GDOŚ jest odpowiedzialny za dokonywanie przeglądu celów SZBI. Przegląd celów jest dokonywany nie rzadziej niż co 12 miesięcy.

3. Monitorowanie realizacji wyznaczonych celów odbywa się na cyklicznych przeglądach zarządzania dokonywanych przez Dyrektora Generalnego GDOŚ.
4. W ramach celów SZBI określane są cele dla poszczególnych ról, procesów i funkcji. Określane cele powinny:
   1) być spójne z PBI;
   2) być mierzalne, określone w czasie oraz wskazujące odpowiedzialnego za realizację danego celu;
   3) uwzględniać aktualne wymagania stron zainteresowanych, w tym czynniki wewnętrzne i zewnętrzne oraz aktualny poziom ryzyka dla poszczególnych zagrożeń;
   4) być monitorowane;
   5) być komunikowane;
   6) w razie potrzeby być aktualizowane.
5. W stosunku do określonych celów należy zdefiniować zadania, które należy zrealizować, aby dany cel został osiągnięty w zaplanowanym czasie.
6. Wyniki monitorowania realizacji celów i wynikających z nich zadań podlegają okresowej analizie i ocenie. Zgodnie z zaplanowanymi ustaleniami oceniane są również uzyskiwane rezultaty zadań. W przypadku negatywnych wyników uruchamiane są odpowiednie działania naprawcze, a w przypadku potrzeby również korygujące.
7. W GDOŚ stosuje się następujące podstawowe zasady dotyczące bezpieczeństwa informacji:
   1) informacja jest jednym z najważniejszych aktywów, dostępnym w wielu różnych formach – na papierze, jako faks lub e-mail, jako słowo mówione, a obecnie przede wszystkim w formie elektronicznej, przetwarzanym z wykorzystaniem urządzeń, aplikacji i systemów teleinformatycznych;
   2) informacje są gromadzone, zapisywane, przechowywane, przetwarzane, oceniane, archiwizowane z wielu różnych źródeł i usuwane lub niszczone zgodnie z wymaganiami prawnymi;
   3) niedostępność, utrata, sfałszowanie lub nieuprawnione ujawnienie nawet części informacji podlegających ochronie może skutkować dużymi szkodami materialnymi lub niematerialnymi dla GDOŚ, niezbędne jest zatem, aby informacje te, niezależnie od ich formy, były chronione odpowiednimi środkami bezpieczeństwa.
8. Celem GDOŚ jest zapewnienie bezpieczeństwa informacji w odpowiednim stopniu przez cały cykl ich życia.
9. W celu określenia rodzaju i zakresu środków ochrony informacji konieczne jest określenie potrzeby ochrony oraz istniejących zagrożeń. Aby to osiągnąć stosuje się proces szacowania ryzyka, w którym bieżąca analiza podatności, zagrożeń i prawdopodobieństwa ich materializacji jest skoordynowana z postępowaniem mającym adekwatne zabezpieczenie informacji.
10. Zapewnienie bezpieczeństwa informacji w szczególności obejmuje:
    1) **poufność** – zapewnienie, że dane nie są udostępniane nieupoważnionym podmiotom;
    2) **integralność** – zapewnienie, aby dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
    3) **dostępność** – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.
11. Zachowanie wszystkich pracowników opiera się na celach bezpieczeństwa informacji i przejawia się w następujących zasadach przewodnich:
    1) każdy, kto przetwarza informacje, odpowiada za ich bezpieczeństwo w ramach wytycznych SZBI;

2) każda informacja musi być sklasyfikowana, zgodnie z zasadami obowiązującymi w GDOŚ;
3) wszelkie informacje podlegające ochronie muszą być zabezpieczone;
4) tylko wyraźnie wskazane osoby posiadające odpowiednie uprawnienia mają dostęp do informacji podlegających ochronie;
5) stosuje się zasadę wiedzy koniecznej, tzn. dostęp do informacji nadawany jest odpowiednio do potrzeb.

12. Wdrożenie zasad przewodnich wymienionych w ust. 12 wymaga wysokiego stopnia świadomości bezpieczeństwa. Kierownictwo GDOŚ aktywnie promuje działania mające na celu uświadomienie pracownikom co oznacza bezpieczeństwo informacji. Podnoszenie świadomości w zakresie bezpieczeństwa informacji oparte jest na 3 filarach:
    1) skutecznego bezpieczeństwa informacji;
    2) stałej świadomości bezpieczeństwa podczas wykonywania wszystkich czynności w pracy;
    3) osobistej odpowiedzialności za zapewnienie bezpieczeństwa informacji w bieżącej realizacji zadań i obowiązków pracowniczych, a także w przypadku wystąpienia incydentu i sytuacji awaryjnych**.**

## § 7. Zgodność z wymaganiami prawnymi

1. Zgodność z przepisami obowiązującego prawa, warunkami przyjętymi w umowach, zapisami odpowiednich norm oraz wewnętrznymi regulacjami jest realizowana poprzez stosowanie poniższych zasad:
    1) identyfikację wymagań prawnych w odniesieniu do bezpieczeństwa informacji;
    2) identyfikację wymagań stron trzecich w odniesieniu do bezpieczeństwa informacji;
    3) wskazanie osób odpowiedzialnych za weryfikację spełnienia wymagań bezpieczeństwa informacji;
    4) prowadzenie audytów wewnętrznych oraz zewnętrznych;
    5) nadzór nad zgodnością stosowanych urządzeń w systemach informatycznych;
2. SZBI w szczególności powinien zapewniać spełnienie wymagań prawnych wynikających z poniższych aktów prawnych:
    1) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2021 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247);
    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);
    3) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
    4) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070, z późn. zm.);
    5) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902);
    6) ustawy z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowiska (Dz. U. z 2022 r. poz. 1129, z późn zm.);

7) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
8) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z późn. zm.);

oraz powinien uwzględniać wymagania zawarte w wewnętrznych aktach prawnych GDOŚ.

**Załącznik nr 2** do Zarządzenia nr 14 Generalnego Dyrektora Ochrony Środowiska w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska z dnia 17 listopada 2022 r.

# *Polityka Przetwarzania Danych Osobowych w Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Generalny Dyrektor Ochrony Środowiska

ANDRZEJ SZWEDA-LEWANDOWSKI

Generalny Dyrektor Ochrony Środowiska .....

Generalny Dyrektor Ochrony Środowiska

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel, zakres oraz podstawa prawna

1. Celem niniejszego dokumentu jest zapewnienie zgodności działania Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ", z obowiązującymi przepisami dotyczącymi ochrony i przetwarzania danych osobowych osób fizycznych oraz zapewnienie należytej ochrony tych danych poprzez opracowanie szczegółowych zasad postępowania i reguł obowiązujących przy przetwarzaniu danych osobowych.
2. Polityka Przetwarzania Danych Osobowych, zwana dalej także „PPDO", ma na celu wdrożenie i realizację działań przy optymalnym wykorzystaniu pozostających w GDOŚ zasobów, środków technicznych i organizacyjnych, które mają zagwarantować odpowiedni poziom bezpieczeństwa w zakresie przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, przetwarzaniem z naruszeniem przepisów oraz przed zmianą, uszkodzeniem, zniszczeniem lub utratą.
3. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   1) poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
   2) integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) dostępności – właściwości zapewniającej, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne;
   4) rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   5) zgodności z prawem – właściwości zapewniającej, że przetwarzane są wyłącznie dane niezbędne do właściwego funkcjonowania jednostki i do których przetwarzania GDOŚ posiada właściwą podstawę prawną przetwarzania o których mowa w art. 6 ust 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia w sprawie ochrony osób fizycznych w związku z przetwarzaniem osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych.
4. Ochrona danych osobowych osób fizycznych jest realizowana w szczególności poprzez:
   1) zabezpieczenia fizyczne (np. kontrola dostępu do pomieszczeń i stref przetwarzania danych);
   2) procedury organizacyjne (np. regulaminy, polityki, zarządzenia dotyczące przetwarzania danych osobowych);
   3) oprogramowanie systemowe (np. zapory typu Firewall, oprogramowanie antywirusowe);
   4) aplikacje (np. oprogramowanie do szyfrowania danych).
5. Szczególne znaczenia dla bezpieczeństwa przetwarzania danych osobowych ma odpowiednie przeszkolenie z zakresu bezpieczeństwa i ochrony danych osobowych pracowników, osób fizycznych z którymi zawarto umowy cywilno-prawne, oraz wolontariuszy i stażystów, którzy realizują zadania związane z przetwarzaniem danych osobowych w GDOŚ.
6. PPDO zakłada pełne zaangażowanie Administratora Danych Osobowych oraz wszystkich pracowników oraz osób współpracujących z GDOŚ w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny (papierowy), jak i przy wykorzystaniu sprzętu oraz systemów informatycznych lub innych nośników informacji.
7. PPDO powinna być aktualizowana wraz ze zmieniającymi się przepisami prawa oraz w związku ze zmianami organizacyjnymi, które powodują, że określone zasady przestają być aktualne.
8. Raz na dwanaście miesięcy PPDO podlega przeglądowi okresowemu, którego zadaniem jest stwierdzenie, czy postanowienia normowane niniejszym dokumentem odpowiadają aktualnemu zakresowi przetwarzania

danych osobowych, obowiązującym procedurom bezpieczeństwa oraz stanowi prawnemu w momencie dokonywania przeglądu.

9. Przeglądu, o którym mowa w ust. 8, dokonują Dyrektorzy Departamentów lub Biur, w zakresie przetwarzanych w podległej komórce organizacyjnej danych osobowych, oraz Inspektor Ochrony Danych i Administrator Bezpieczeństwa Teleinformatycznego. W przypadku, gdy wyniki przeglądu wskazują na konieczność aktualizacji PPDO, osoby, o których mowa w poprzednim zdaniu, informują o tym fakcie Administratora Danych Osobowych, który może podjąć działania mające na celu aktualizację PPDO lub dokumentów z nią powiązanych.
10. Przy aktualizacji procedur bezpieczeństwa zawartych w PPDO należy uwzględnić przypadki występowania naruszeń zasad postępowania z danymi osobowymi. Jeżeli z analizy występujących i powtarzających się incydentów naruszenia bezpieczeństwa związanych z ochroną danych osobowych wynika, że są one rezultatem rozwiązań systemowych, w szczególności błędnych procedur, powinna nastąpić zmiana procedur i zasad przetwarzania danych osobowych oraz aktualizacja dokumentacji dotyczącej przetwarzania danych osobowych w zakresie niezbędnym do eliminacji lub ograniczenia prawdopodobieństwa wystąpienia w przyszłości podobnych naruszeń.
11. Aktualizacje i zmiany PPDO zatwierdza Administrator Danych Osobowych.
12. Sposób zarządzania systemem informatycznym, ze szczególnym uwzględnieniem zapewnienia jego bezpieczeństwa, określa Polityka Bezpieczeństwa Teleinformatycznego, stanowiąca odrębny dokument.
13. PPDO obowiązująca w GDOŚ, została opracowana na podstawie niżej wymienionych przepisów prawa oraz wytycznych zawartych w następujących aktach prawnych:
    1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 Nr 119 z 2016 r., s.1);
    2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781).
14. Przetwarzanie danych osobowych w GDOŚ odbywa się na podstawie przepisów obowiązującego prawa. Przepisami sektorowymi upoważniającymi GDOŚ do przetwarzania danych osobowych są w szczególności przepisy:
    1) ustawy z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz.U. z 2022 r. poz. 1029, ze zm.);
    2) ustawy z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska (Dz. U. z 2021 r. poz. 1973, z późn. zm.);
    3) ustawy z dnia 16 kwietnia 2004 r. o ochronie przyrody (Dz. U. z 2022 r. poz. 916, z późn. zm.);
    4) ustawy z dnia 13 kwietnia 2007 r. o zapobieganiu szkodom w środowisku i ich naprawie (Dz. U. z 2020 r. poz. 2187);
    5) ustawy z dnia 15 lipca 2011 r. o krajowym systemie ekozarządzania i audytu (EMAS) (Dz. U. z 2020 r. poz. 634);
    6) ustawy z dnia 11 sierpnia 2021 o gatunkach obcych (Dz.U.2021 poz. 1718);
    7) ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2022 r. poz. 1510, ze zm.);
    8) ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2022 r. poz. 1009, ze zm.);
    9) ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. 2022 r. poz. 1691).

## § 2. Terminologia

1. Pojęcia używane w niniejszym dokumencie oraz innych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji są zdefiniowane w dokumencie ***Słownik pojęć używanych w dokumentach Systemu Zarządzania Bezpieczeństwem Informacji Generalnej Dyrekcji Ochrony Środowiska***.
2. Ilekroć w treści niniejszego dokumentu jest mowa o:
   1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ;
   2) **Administratorze Danych Osobowych** (**ADO**) – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem Danych Osobowych jest Generalny Dyrektor Ochrony Środowiska, w imieniu którego zadania realizuje Dyrektor Generalny GDOŚ. W zakresie przetwarzania danych osobowych osób zatrudnionych w GDOŚ Administratorem Danych Osobowych jest Generalna Dyrekcja Ochrony Środowiska w imieniu której funkcję ADO wykonuje Dyrektor Generalny GDOŚ;
   3) **anonimizacji danych osobowych** – należy przez to rozumieć proces przekształcenia danych (dokumentu) uniemożliwiający odkrycie (ustalenie) tożsamości osoby fizycznej;
   4) **danych o stanie zdrowia** – należy przez to rozumieć dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie zdrowia (np. informacja o korzystaniu z lub leczeniu w poradni zdrowia psychicznego);
   5) **danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
   6) **Departamencie lub Biurze** – należy przez to rozumieć komórki organizacyjne i stanowiska wymienione w § 3 ust. 1 statutu Generalnej Dyrekcji Ochrony Środowiska stanowiącego załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 12 listopada 2008 r. w sprawie nadania statutu Generalnej Dyrekcji Ochrony Środowiska (Dz. U. z 2015 r. poz. 1350 i z 2016 r., poz. 1380);
   7) **dokumentacji przetwarzania danych** – należy przez to rozumieć dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Na dokumentację przetwarzania danych w GDOŚ, w szczególności składa się Polityka Przetwarzania Danych Osobowych, Polityka Bezpieczeństwa Informacji i Polityka Bezpieczeństwa Teleinformatycznego;
   8) **Dyrektorze Departamentu lub Biura –** należy przez to rozumieć dyrektora departamentu albo biura, jego zastępcę lub inną osobę wyznaczoną do kierowania komórką organizacyjną;
   9) **haśle** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

10) **identyfikatorze** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 RODO, którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 RODO;
12) **Kierującym zespołem** – należy przez to rozumieć kierowników zespołów albo naczelników wydziałów wchodzących w skład Departamentów lub Biur;
13) **naruszeniu ochrony danych osobowych** – należy przez to rozumieć 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;
14) **odbiorcy** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców. Przetwarzanie tych danych przez organy publiczne musi być zgodne z przepisami o ochronie danych mających zastosowanie stosownie do celów przetwarzania;
15) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego wykorzystania;
16) **osobie przetwarzającej dane** – należy rozumieć osobę wykonującą pracę w ramach stosunku pracy lub świadczącą usługi na podstawie umowy cywilnoprawnej, osobę odbywającą staż lub realizującą zadania w formie wolontariatu w GDOŚ, która uzyskała upoważnienie do przetwarzania danych osobowych. Wzór upoważnienia określa załącznik nr 7 do Polityki Przetwarzania Danych Osobowych;
17) **podmiocie przetwarzającym** – należy przez to rozumieć osobę fizyczną prowadzącą działalność gospodarczą lub osobę prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych na podstawie umowy powierzenia danych osobowych lub innego instrumentu prawnego;
18) **Polityce Bezpieczeństwa Teleinformatycznego** – należy przez to rozumieć dokument opisujący minimalne wymagania dla systemów teleinformatycznych GDOŚ;
19) **poufności danych** – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
20) **profilowaniu** – należy przez to rozumieć dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. W szczególności do analizy lub prognozy dotyczących efektów pracy osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
21) **przetwarzaniu danych** – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, przeglądanie, utrwalanie organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

22) **publicznej sieci telekomunikacyjnej** — należy przez to rozumieć sieć telekomunikacyjną w rozumieniu art. 2 pkt. 29 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (Dz. U. 2022 poz. 1648);

23) **Rejestrze Czynności Przetwarzania** – należy przez to rozumieć rejestr prowadzony przez Administratora Danych Osobowych, w którym zamieszcza się następujące dane: nazwę i dane Administratora Danych Osobowych oraz wszystkich współadministratorów oraz Inspektora Ochrony Danych; cele przetwarzania; opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych; kategorie odbiorców, którym dane osobowe zostały ujawnione; jeśli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; jeśli jest to możliwe ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Wzór Rejestru, opracowany na podstawie art. 30 ust. 1 RODO, określa załącznik nr 1 do Polityki Przetwarzania Ochrony Danych Osobowych. Rejestr może być prowadzony w formie papierowej lub elektronicznej;

24) **Rejestrze Kategorii Czynności Przetwarzania** – należy przez to rozumieć rejestr prowadzony przez podmiot przetwarzający, zawierający wszystkie kategorie czynności przetwarzania dokonywane w imieniu administratora. Rejestr zawiera: nazwę podmiotu przetwarzającego, nazwę administratora w imieniu którego działa podmiot przetwarzający, dane inspektora ochrony danych, kategorie przetwarzań dokonywanych w imieniu każdego z administratorów; informacje o przekazywaniu danych do państwa trzeciego; ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Wzór Rejestru, opracowany na podstawie art. 30 ust. 2 RODO, określa załącznik nr 2 do Polityki Przetwarzania Danych Osobowych. Rejestr może być prowadzony w formie papierowej lub elektronicznej;

25) **Rejestrze Naruszeń** – należy przez to rozumieć rejestr zawierający opis stwierdzonych w GDOŚ naruszeń ochrony danych, opis czynności podjętych w celu zapobieżenia negatywnym skutkom dla praw i wolności osób fizycznych, których dane zostały ujawnione, zniszczone lub zmienione w wyniku naruszenia zasad bezpieczeństwa, informację o zawiadomieniu lub nie zawiadomieniu organu nadzorczego. Wzór Rejestru określa załącznik nr 2 do Procedury zarządzania incydentami bezpieczeństwa informacji, w tym danych osobowych w GDOŚ, która stanowi odrębny dokument;

26) **Rejestrze Nośników Danych** – należy przez to rozumieć rejestr prowadzony przez Kierującego zespołem do spraw informatyki lub innego wyznaczonego pracownika zespołu do spraw informatyki, zawierający informacje dotyczące zasobów informatycznych wykorzystywanych jako nośniki danych. Rejestr zawiera zarówno informacje dotyczące nośników danych zainstalowanych w urządzeniach stacjonarnych oraz mobilnych (dyski i pamięć wewnętrzna) jak również pamięci masowych oraz nośników optycznych (pendrive, płyty CD, DVD itp.) Wzór Rejestru określa załącznik nr 4 do Polityki Przetwarzania Danych Osobowych. Rejestr może być prowadzony w formie papierowej lub elektronicznej;

27) **Rejestrze Osób Upoważnionych do Przetwarzania Danych Osobowych** – należy przez to rozumieć rejestr zawierający ewidencję osób, którym Administrator Danych Osobowych danych wydał upoważnienie do przetwarzania w jego imieniu danych osobowych. Wzór Rejestru określa załącznik nr 6 do Polityki Przetwarzania Danych Osobowych. Rejestr może być prowadzony w formie papierowej lub elektronicznej;

28) **Rejestrze Umów Powierzenia** – należy przez to rozumieć rejestr zawierający wykaz podmiotów, którym Administrator Danych Osobowych powierzył w niezbędnym zakresie, przetwarzanie danych osobowych w związku z realizacją, w jego imieniu i na jego zlecenie, zadań przez te podmioty. Rejestr zawiera nazwę podmiotu, któremu Administrator Danych Osobowych powierzył przetwarzanie danych osobowych, okres obowiązywania umowy, zakres powierzonych danych, cel powierzenia. Rejestr prowadzi Przedstawiciel Administratora Danych Osobowych. Wzór rejestru określa załącznik nr 3 do Polityki Przetwarzania Danych Osobowych. Rejestr może być prowadzony w formie papierowej lub elektronicznej;

29) **Rejestrze Zapytań i Wniosków** – należy przez to rozumieć rejestr zawierający ewidencję wniosków i zapytań skierowanych przez osoby fizyczne na podstawie art. 15-21 RODO do Administratora Danych Osobowych w związku z przetwarzaniem ich danych osobowych. Rejestr prowadzi Przedstawiciel Administratora Danych Osobowych. Wzór rejestru określa załącznik nr 5 do Polityki Przetwarzania Danych Osobowych. Rejestr może być prowadzony w formie papierowej lub elektronicznej;

30) **RODO** – należy przez to rozumieć Rozporządzenie 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);

31) **sieci telekomunikacyjnej** — należy przez to rozumieć sieć telekomunikacyjną w rozumieniu art. 2 pkt. 34 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne;

32) **sprawdzeniu** – należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

33) **sprawozdaniu** – należy przez to rozumieć dokument, opracowany przez Inspektora Ochrony Danych w związku z realizowaniem obowiązku wynikającego z art. 39 ust. 1 lit. b RODO;

34) **strefie przetwarzania danych** – należy przez to rozumieć zespół pomieszczeń w których realizuje się zadania z zakresu przetwarzania danych osobowych;

35) **zgodzie** – należy przez to rozumieć dobrowolne, konkretne, świadome i jednoznaczne wyrażenie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

## § 3. Obowiązki Administratora Danych Osobowych (ADO)

1. Zgodnie z art. 24 i 25 RODO ADO przetwarzający dane ma obowiązek dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
   1) przetwarzane zgodnie z prawem;
   2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu i wykorzystywaniu w sposób niezgodny z tymi celami;
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
   5) archiwizowane i usuwane (kasowane) po dopuszczalnym prawem okresie przetwarzania lub w przypadku osiągnięcia wszystkich celów, dla których były przetwarzane.
2. Na ADO ciąży obowiązek zastosowania, stosownych do poziomu ryzyka, rozwiązań technicznych i organizacyjnych gwarantujących bezpieczeństwo przetwarzania danych osobowych, zgodność przetwarzania z obowiązującymi przepisami prawa oraz rozliczalność na każdym etapie procesów przetwarzania, w szczególności pod kątem dostępu do danych, dostępu do pomieszczeń, w których realizowany jest proces przetwarzania, i systemów informatycznych wykorzystywanych w GDOŚ.
3. ADO ma obowiązek okresowego przeglądu i uaktualnienia zastosowanych procedur bezpieczeństwa przetwarzania.

4. ADO realizuje obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. ADO ma również obowiązek zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem, nielegalnym przetwarzaniem, zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. Obowiązkiem ADO jest zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe, oraz środków niezbędnych do zapewnienia, adekwatnego do stopnia zagrożenia, poziomu bezpieczeństwa danych przetwarzanych w systemach informatycznych.
6. Obowiązkiem ADO jest zapewnienie takich rozwiązań organizacyjnych, które gwarantują, że IOD jest właściwie i niezwłocznie włączony we wszystkie sprawy dotyczące ochrony danych osobowych.
7. W zakresie ochrony danych przetwarzanych w formie tradycyjnej (tj. w formie papierowej) zabezpieczenie danych w GDOŚ realizowane jest poprzez:
    1) przechowywanie dokumentów w pomieszczeniach o ograniczonym dostępie osób trzecich;
    2) stałe podnoszenie poziomu wiedzy i świadomości na temat ochrony danych osobowych poprzez regularne szkolenia i podnoszenie kwalifikacji osób przetwarzających dane osobowe;
    3) ograniczenie do niezbędnego minimum kręgu osób posiadających dostęp do danych osobowych oraz pomieszczeń, w których są one przetwarzane i przechowywane;
    4) zapewnienie rozliczalności dostępu do danych osobowych poprzez stosowanie zasad ewidencjonowania obiegu dokumentów i dostępu do pomieszczeń biurowych;
    5) wprowadzenie systemu upoważnień do przetwarzania danych osobowych;
    6) stosowanie zamykanych na klucz pomieszczeń i szaf, w których przechowywane są dane osobowe;
    7) wprowadzenie zasad umożliwiających rozliczalność dostępu do pomieszczeń, w których przetwarzane są dane osobowe, w szczególności systemu upoważnień i ewidencjonowania dostępu do pomieszczeń;
    8) wprowadzanie wytycznych do postępowania z dokumentacją zawierająca dane chronione, w tym egzekwowanie zasady tzw. „czystego biurka”;
    9) okresowe przeglądy danych i dokumentów podlegających archiwizacji lub usunięciu na podstawie przepisów ustawy z dnia z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164, ze. zm.).
8. Zasady dotyczące bezpieczeństwa systemów teleinformatycznych zostały określone w Polityce Bezpieczeństwa Teleinformatycznego.
9. Obowiązek ADO dopuszczenia do przetwarzania danych osobowych wyłącznie osób upoważnionych realizowany jest poprzez:
    1) odpowiednie przeszkolenie pracowników oraz wydanie im stosownego upoważnienia do przetwarzania danych osobowych;
    2) szkolenie i upoważnienie, o którym mowa w pkt 1, dotyczy osób zatrudnionych w GDOŚ na podstawie umów o pracę, osób fizycznych realizujących zadania na podstawie umów cywilnoprawnych, stażystów oraz wolontariuszy, o ile z zakresu obowiązków lub postanowień zawartych z nimi umów wynika, że do realizacji powierzonych zadań niezbędny jest dostęp do danych osobowych;
    3) prowadzenie Rejestru Osób Upoważnionych do Przetwarzania Danych Osobowych; Rejestr ten zawiera:
        a) imię i nazwisko osoby upoważnionej,
        b) datę nadania i ustania upoważnienia,
        c) zakres upoważnienia wynikający z Rejestru czynności przetwarzania i zakresu obowiązków.

10. Obowiązkiem ADO jest wdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zapewnienie by przetwarzanie danych odbywało się zgodnie z RODO. ADO powinien móc wykazać, że zastosował odpowiednie rozwiązania techniczne i organizacyjne. W tym celu ADO wdrożył System Zarządzania Bezpieczeństwem Informacji zgodny z normą ISO/IEC 27001, zawierający dokumenty opisujące sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne. Dokumentacja w szczególności powinna zawierać:
    1) Politykę przetwarzania danych osobowych;
    2) Politykę bezpieczeństwa teleinformatycznego;
    3) Rejestr Czynności Przetwarzania;
    4) Rejestr Kategorii Czynności Przetwarzania;
    5) Rejestr Umów Powierzenia;
    6) Rejestr Osób Upoważnionych do Przetwarzania Danych Osobowych;
    7) Rejestr Naruszeń;
    8) Rejestr Zapytań i Wniosków.

## § 4. Obowiązki Inspektora Ochrony Danych Osobowych (IOD), osób funkcyjnych przetwarzających dane osobowe oraz Przedstawiciela Administratora Danych Osobowych

1. Zgodnie z RODO obowiązkiem ADO będącego jednostką administracji publicznej jest powołanie Inspektora Ochrony Danych. Jeśli jest to uzasadnione potrzebami i strukturą organizacyjną, ADO na podstawie art. 11a Ustawy z 10 maja 2018 r. o ochronie danych osobowych może powołać Zastępcę Inspektora Ochrony Danych.
2. Inspektor Ochrony Danych (IOD) oraz Zastępcy Inspektora Ochrony Danych powoływani i odwoływani są przez Administratora Danych Osobowych.
3. IOD oraz jego Zastępca podlegają zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych jako organu nadzorczego do spraw ochrony danych osobowych.
4. Do zadań IOD i jego Zastępcy należy:
    1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO;
    2) bieżące informowanie ADO, pracowników zatrudnionych w GDOŚ, osób fizycznych realizujących zadania dla GDOŚ na podstawie umów cywilnoprawnych, stażystów oraz wolontariuszy o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych oraz przepisów UE w tym zakresie;
    3) monitorowanie przestrzegania przepisów prawa w zakresie ochrony danych osobowych oraz przepisów UE i innych przepisów o ochronie danych oraz polityki ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz prowadzenie audytów i sprawdzeń w tym zakresie;
    4) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych i środki techniczne oraz organizacyjne zapewniające ich ochronę, a także przestrzegania zasad w niej określonych;
    5) na wniosek Prezesa Urzędu Ochrony Danych Osobowych– dokonanie sprawdzenia zgodności, sposobu oraz zakresu przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

6) po dokonaniu sprawdzenia, o którym mowa w pkt. 5 – opracowanie sprawozdania, które z pominięciem ADO przekazywane jest do Prezesa Urzędu Ochrony Danych Osobowych;
7) udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
8) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe, oraz kontrola przebywających w nich osób;
9) udzielanie zaleceń ADO mających znaczenie dla ochrony danych oraz monitorowanie ich wykonania;
10) współpraca z organem nadzorczym ds. ochrony danych osobowych, w tym pełnienie funkcji punktu kontaktowego/konsultacyjnego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych;
11) uczestniczenie w pracach Zespołu.

5. ABT wyznaczony przez ADO powinien zapoznać się z dokumentem PPDO. Zakres odpowiedzialności ABT określony jest w Polityce Bezpieczeństwa Teleinformatycznego.
6. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych od ADO, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, opracowanej i wdrożonej w GDOŚ dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, m.in. zasad postępowania z dokumentami w formie tradycyjnej oraz zasad postępowania w przypadku nieuprawnionego ujawnienia danych osobowych lub innego incydentu związanego z bezpieczeństwem danych osobowych. Każde naruszenie ochrony danych osobowych powinno być zgłaszane zgodnie z **Procedurą zarządzania incydentami bezpieczeństwa informacji, w tym danych osobowych w GDOŚ**, stanowiącą odrębny dokument.
7. Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zachowania w tajemnicy tych danych osobowych, do których w ramach wykonywanych obowiązków uzyskała dostęp, oraz sposobów zabezpieczenia danych osobowych i procedur obowiązujących w GDOŚ w powyższym zakresie. Obowiązek ten istnieje również po ustaniu zatrudnienia.
8. W przypadku zawinionego naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej. Naruszenie zasad ochrony danych osobowych, a także sposobu ich zabezpieczania może skutkować postawieniem pracownikowi zarzutu popełnienia przestępstwa określonego w art. 266 Kodeksu Karnego.
9. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek aktywnie uczestniczyć w tworzeniu i modyfikacji procedur i rozwiązań technicznych mających na celu poprawę bezpieczeństwa i reagowania na zagrożenie dla danych osobowych. Przez aktywne uczestnictwo rozumie się między innymi:
    1) zgłaszanie przełożonym, IOD lub ABT zaobserwowanych problemów i słabych punktów w systemie ochrony danych;
    2) reagowanie na zagrożenia dla poufności, integralności, dostępności i bezpieczeństwa danych.
10. W celu ochrony danych, osoby upoważnione do przetwarzania danych osobowych podczas ich przetwarzania winny uwzględniać następujące zasady:
    1) chronić dane osobowe przed przechwyceniem, kopiowaniem, modyfikacją lub zniszczeniem;
    2) przestrzegać zakazu pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, do których mogą mieć dostęp osoby nieupoważnione;
    3) nie korzystać z punktów usługowych ksero lub innych publicznych urządzeń służących do kopiowania dokumentów, jeśli kopiowane dokumenty zawierają dane osobowe lub inne dane podlegające ochronie;

4) weryfikować tożsamość rozmówcy w trakcie rozmów telefonicznych i ustalać, czy rozmówca jest osobą upoważnioną do uzyskania określonych informacji. Tożsamość rozmówcy można zweryfikować poprzez zadanie dodatkowych pytań, np. o datę urodzenia, drugie imię, imiona rodziców itp. W przypadku braku możliwości weryfikacji tożsamości rozmówcy, należy odmówić udzielenia żądanych informacji;
5) weryfikować tożsamość rozmówcy przy osobistym kontakcie, w celu potwierdzenia uprawnień do uzyskania informacji, poprzez sprawdzenie dokumentu tożsamości ze zdjęciem;
6) zachować szczególną ostrożność w trakcie rozmów telefonicznych;
7) nie pozostawiać wiadomości zawierających dane osobowe na automatycznych sekretarkach.

11. W zakresie dotyczącym ochrony danych osobowych obowiązkiem Dyrektorów Departamentów lub Biur jest:
    1) dokonywanie okresowych, nie rzadziej niż raz na 12 miesięcy, przeglądów kategorii przetwarzanych danych osobowych przez podległych pracowników, pod kątem, zgodności i aktualności przetwarzanych danych;
    2) jeśli jest to konieczne – aktualizacja Rejestru Czynności Przetwarzania oraz Rejestru Kategorii Czynności Przetwarzania Danych Osobowych w zakresie, w jakim dotyczy spraw danej komórki organizacyjnej;
    3) niezwłoczne zgłaszanie i konsultowanie z IOD konieczności zmian w dokumentacji i procedurach dot. ochrony danych osobowych;
    4) stała współpraca z IOD w zakresie przetwarzania danych osobowych, w tym w szczególności określaniu legalności, celowości i niezbędności gromadzonych i przetwarzanych danych;
    5) informowanie IOD o nowo zatrudnionych pracownikach, wymagających przeszkolenia z zakresu ochrony danych osobowych;
    6) opracowanie wniosków o nadanie, zmianę lub cofnięcie upoważnień do przetwarzania danych osobowych i uzyskania dostępu do zasobów informatycznych GDOŚ;
    7) bieżący nadzór i kontrola na podległym personelem w zakresie przestrzegania przez niego zasad i przepisów dotyczących ochrony danych osobowych.
12. Dyrektorzy Departamentów lub Biur raz na 12 miesięcy, przy wsparciu IOD, przeprowadzają szacowanie ryzyka przetwarzania danych osobowych zgodnie z ***Procedurą zarządzania ryzykiem wraz z metodyką szacowania ryzyka GDOŚ***, która stanowi odrębny dokument, i na tej podstawie przedstawiają ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych celem zapewnienia właściwej ochrony przetwarzanych danych osobowych oraz wdrożenia odpowiednich mechanizmów nadzoru i kontroli.
13. Przeprowadzenie oceny skutków przetwarzania dla ochrony danych osobowych jest obowiązkowe każdorazowo przed rozpoczęciem przetwarzania nowej kategorii danych lub przy planowanym przetwarzaniu danych na dużą skalę.
14. Analizę ryzyka przeprowadza się na zasadach i przy użyciu metodologii określonej w ***Procedurze zarządzania ryzykiem wraz z metodyką szacowania ryzyka w GDOŚ***.
15. Dyrektorzy Departamentów lub Biur są odpowiedzialni za uzyskanie opinii IOD w sprawie zakresu powierzenia danych osobowych podmiotom zewnętrznym realizującym zadania na rzecz GDOŚ, o ile powierzenie danych jest niezbędne do prawidłowej realizacji zleconych zadań lub umowy o świadczenie usług. Opinię należy uzyskać przed faktycznym udostępnieniem danych, w terminie umożliwiającym opracowanie i zawarcie stosownej umowy o powierzeniu przetwarzania danych osobowych.
16. Dyrektorzy Departamentów lub Biur są odpowiedzialni za uzyskanie opinii IOD w sprawie realizacji wniosków osób fizycznych dotyczących realizacji praw o których mowa w art. 15-21 RODO.

17. Dyrektor Generalny GDOŚ w celu organizacji, koordynacji i nadzoru nad przetwarzaniem danych osobowych w GDOŚ powołuje swojego Przedstawiciela.
18. Przedstawiciel Administratora Danych Osobowych, o którym mowa w ust. 17, w zakresie dotyczącym danych osobowych jest odpowiedzialny za:
    1) prowadzenie Rejestru Osób Upoważnionych do Przetwarzania Danych Osobowych;
    2) opracowanie, na podstawie otrzymanych wniosków, projektów upoważnień do przetwarzania danych osobowych;
    3) prowadzenie Rejestru Umów Powierzenia;
    4) prowadzenie Rejestru Zapytań i Wniosków;
    5) prowadzenie Rejestru Naruszeń;
    6) nadzór nad przetwarzaniem danych osobowych w GDOŚ,
    7) decyzję o przekazaniu danych osobowych do państwa trzeciego;
    8) organizację szkoleń z zakresu ochrony danych osobowych;
    9) nadzór realizacji obowiązków informacyjnych o których mowa w art. 13 i 14 RODO;
    10) nadzór nad aktualizacją Rejestru Czynności Przetwarzania i Rejestru Kategorii Czynności Przetwarzania.
19. Przedstawiciel Administratora Danych Osobowych, o którym mowa w ust. 17, przy realizacji powierzonych mu zadań ściśle współpracuje z IOD.

## § 5. Upoważnienia do przetwarzania danych osobowych, Rejestr Osób Upoważnionych do Przetwarzania Danych Osobowych oraz szkolenia z zakresu ochrony danych osobowych

1. Upoważnienie do przetwarzania danych osobowych wydawane jest pracownikom GDOŚ zatrudnionym na podstawie umowy o pracę, osobom fizycznym wykonującym zadania na rzecz GDOŚ na podstawie umowy cywilnoprawnej, stażystom oraz wolontariuszom – jeśli z treści umowy o pracę, umowy cywilnoprawnej lub umowy o staż, praktyki lub wolontariat wynika, iż dostęp do danych osobowych przetwarzanych w GDOŚ jest im niezbędny do realizacji zadań objętych tą umową.
2. Upoważnienie do przetwarzania danych osobowych wydawane jest na wniosek Dyrektora Departamentu lub Biura właściwego ze względu na miejsce realizacji zadań osoby upoważnionej.
3. Wniosek o wydanie upoważnienia do przetwarzania danych osobowych jest integralną częścią wniosku o nadanie uprawnień do systemów teleinformatycznych, który opracowuje się na podstawie zakresu obowiązków na zajmowanym stanowisku pracy oraz Rejestru Czynności Przetwarzania.
4. Jeżeli wynika to z zakresu obowiązków i sposobu przetwarzania danych osobowych, wniosek o wydanie upoważnienia do przetwarzania danych osobowych powinien zawierać niezbędny zakres dostępu do zasobów informatycznych GDOŚ. Wzór wniosku zawiera załącznik nr 9 do Polityki Przetwarzania Danych Osobowych.
5. Wniosek o wydanie upoważnienia do przetwarzania danych osobowych oraz nadania uprawnień dostępu do zasobów informatycznych GDOŚ może mieć formę elektroniczną i być przesyłany za pomocą wewnętrznej sieci teleinformatycznej (intranet, EZD).
6. Upoważnienie do przetwarzania danych osobowych zawiera w szczególności:
    1) imię i nazwisko osoby upoważnionej;
    2) numer upoważnienia;

3) stanowisko służbowe;
4) datę wydania upoważnienia;
5) datę ważności upoważnienia (w przypadku umów na czas określony);
6) zakres dostępu do danych osobowych, zgodnie z Rejestrem Czynności Przetwarzania;
7) informacje o unieważnieniu poprzedniego upoważnienia, o ile zostało wydane;
8) podpis osoby wydającej upoważnienie (Administratora Danych Osobowych lub osoby upoważnionej);
9) podpis osoby upoważnionej.

7. Upoważnienie do przetwarzania danych osobowych wydawane jest po zapoznaniu się przez osobę upoważnioną z:
   1) przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   2) przepisami RODO;
   3) obowiązującymi w GDOŚ zasadami przetwarzania i ochrony danych osobowych.
8. Zapoznanie osoby upoważnionej do przetwarzania danych osobowych z dokumentami o których mowa w ust. 7, może nastąpić poprzez wewnętrzną sieć teleinformatyczną (intranet, EZD).
9. Osoba upoważniona do przetwarzania danych osobowych składa oświadczenie o zapoznaniu się z dokumentami, o których mowa w ust. 7. Wzór oświadczenia osoby upoważnionej zawiera załącznik nr 8 do Polityki Przetwarzania Danych Osobowych.
10. Upoważnienie do przetwarzania danych osobowych wydawane jest w dwóch jednobrzmiących egzemplarzach. Jeden egzemplarz upoważnienia wydaje się osobie upoważnionej. Drugi egzemplarz wraz z oświadczeniem osoby upoważnionej o zapoznaniu się z dokumentami, o których mowa w ust. 7, oraz oświadczeniem o obowiązku zachowania poufności, dołącza się do dokumentacji kadrowej pracownika prowadzonej przez komórkę kadrową GDOŚ.
11. Upoważnienie do przetwarzania danych osobowych cofa się lub zmienia na wniosek Dyrektora Departamentu lub Biura właściwego ze względy na miejsce realizacji zadań osoby upoważnionej w przypadku:
   1) rozwiązania lub wygaśnięcia umowy o pracę lub umowy cywilnoprawnej przed okresem na który została zawarta;
   2) zmiany stanowiska pracy lub zakresu obowiązków, z którym wiąże się zmiana sposobu lub zakresu przetwarzania danych osobowych;
   3) powtarzających się i potwierdzonych przypadków nieprzestrzegania zasad bezpieczeństwa przetwarzania i ochrony danych osobowych;
   4) potwierdzonego, umyślnego i bezprawnego kopiowania, ujawniania, powielania lub udostępniania danych osobowych.
12. W przypadkach określonych w ust. 11 pkt. 3 i 4 wniosek o cofnięcie upoważnienia do przetwarzania danych osobowych może złożyć IOD lub ABT.
13. Cofnięcie upoważnienia do przetwarzania danych osobowych, z powodów o których mowa w ust. 11 pkt 3 i 4, może skutkować rozwiązaniem umowy o pracę lub umowy cywilnoprawnej z przyczyn leżących po stronie pracownika lub zleceniobiorcy.
14. W GDOŚ prowadzi się Rejestr Osób Upoważnionych do Przetwarzania Danych Osobowych.
15. Rejestr Osób Upoważnionych do Przetwarzania Danych Osobowych prowadzi z zachowaniem zasad chronologii i kolejności dokonywania wpisów Przedstawiciel Administratora Danych Osobowych.

16. Rejestr Osób Upoważnionych do Przetwarzania Danych Osobowych zawiera w szczególności:
    1) numer upoważnienia;
    2) imię i nazwisko osoby upoważnionej;
    3) datę wydania upoważnienia;
    4) datę ważności upoważnienia;
    5) stanowisko służbowe osoby upoważnionej;
    6) zakres upoważnienia;
    7) datę odbycia przez osobę upoważnioną przeszkolenia z zakresu ochrony danych osobowych.
17. Rubryka określająca datę ważności upoważnienia, znajdująca się w Rejestrze Osób Upoważnionych do Przetwarzania Danych Osobowych dotyczy upoważnień wydanych pracownikom zatrudnionym na czas określony lub osobom realizującym zadania w ramach umowy cywilnoprawnej zawartej na czas oznaczony. W przypadku umów o pracę na czas nieokreślony lub umów cywilnoprawnych zawartych na czas nieoznaczony można stosować zapis „do odwołania”.
18. W rubryce określającej zakres upoważnienia, znajdującej się w Rejestrze Osób Upoważnionych do Przetwarzania Danych Osobowych, umieszcza się wszystkie realizowane przez osobę upoważnioną czynności przetwarzania danych osobowych, zgodnie z nazewnictwem i zawartością Rejestru Czynności Przetwarzania.
19. Osoby, którym zostanie wydane upoważnienie do przetwarzania danych osobowych, objęte są obowiązkiem odbycia szkolenia z zakresu przepisów prawa dotyczących ochrony danych osobowych oraz procedur bezpieczeństwa danych osobowych obowiązujących w GDOŚ.
20. Szkolenia z zakresu ochrony danych osobowych prowadzi IOD lub jego Zastępca. Realizację tych szkoleń można także powierzyć podmiotom zewnętrznym. Dokumentem potwierdzającym odbycie szkolenia jest imienne zaświadczenie.
21. Jeśli jest to uzasadnione warunkami technicznych, epidemiologicznych lub ekonomicznych, szkolenia z zakresu ochrony danych osobowych mogą być przeprowadzone w formie telekonferencji.
22. IOD wydaje osobom, które przeszkolił, zaświadczenie o odbyciu szkolenia z zakresu ochrony danych osobowych. W przypadku szkoleń zrealizowanych przez podmioty zewnętrzne, umowy zawierane przez GDOŚ z takimi podmiotami powinny przewidywać obowiązek wydawania przez te podmioty stosownych zaświadczeń dla uczestników szkoleń.
23. Zaświadczenie, o którym mowa w ust. 22, przechowuje się w dokumentacji kadrowej pracownika prowadzonej przez komórkę kadrową GDOŚ.
24. Szkolenia dla nowozatrudnionych pracowników odbywają się raz na 90 dni i dotyczą wszystkich nowo zatrudnionych pracowników, o ile z zakresu obowiązków na zajmowanym stanowisku pracy wynika, że będą oni przetwarzać dane osobowe.
25. W terminie 90 dni od wejścia w życie Zarządzenia Dyrektora Generalnego GDOŚ wprowadzającego „Politykę Przetwarzania Danych Osobowych”, Inspektor Ochrony Danych Osobowych lub Zastępca Inspektora Ochrony Danych przeprowadzą szkolenia dla całego personelu GDOŚ.
26. Szkolenia można powtórzyć w przypadku zmiany przepisów prawa dotyczącego ochrony danych osobowych lub istotnych zmian procedur bezpieczeństwa przetwarzania danych osobowych obowiązujących w GDOŚ. Decyzję w tym zakresie podejmuje Administrator Danych Osobowych.
27. Pracownicy GDOŚ zobowiązani są, w ramach samokształcenia, do systematycznego uzupełniania i aktualizowania posiadanej wiedzy z zakresu ochrony danych osobowych.

## § 6. Powierzenie i współadministrowanie danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z jednostką mają dostęp do danych osobowych przetwarzanych w jednostce.
2. Dane osobowe mogą być powierzone jedynie podmiotom, które wdrożyły odpowiednie środki techniczne i organizacyjne gwarantujące bezpieczne i zgodne z przepisami prawa przetwarzanie danych osobowych oraz ochronę praw osób, których dane dotyczą.
3. Wykonawcy biorących udział w postępowaniach i konkursach, w tym także prowadzonych na podstawie przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, których przedmiotem jest dostawa towarów lub usług, lub wykonanie robót budowlanych, z którymi wiąże się konieczność powierzenia im danych osobowych, składają wraz z ofertą, lub wnioskiem o dopuszczenie do udziału w postępowaniu lub w konkursie, oświadczenia zawierające informacje o:
   1) wprowadzeniu odpowiednich rozwiązań organizacyjnych i technicznych gwarantujących bezpieczeństwo danych osobowych;
   2) posiadaniu upoważnionego i przeszkolonego z zakresu ochrony danych osobowych personelu;
   3) prowadzeniu Rejestru Kategorii Czynności Przetwarzania;
   4) dane kontaktowe Inspektora Ochrony Danych – o ile został powołany.

   Informacje o obowiązku złożenia oświadczeń dotyczących bezpieczeństwa danych osobowych umieszcza się w Specyfikacji Warunków Zamówienia (SWZ) lub zaproszeniu do złożenia oferty.

   Wzór oświadczenia wykonawcy zawiera załącznik nr 10 do Polityki Przetwarzania Danych Osobowych.
4. Administrator Danych Osobowych powierzy przetwarzanie danych osobowych podmiotom zewnętrznym jedynie w zakresie niezbędnym do prawidłowego wykonania zadań realizowanych przez te podmioty na rzecz Administratora Danych Osobowych.
5. Powierzenie może mieć miejsce wyłącznie w trybie przewidzianym przepisami art. 28 RODO poprzez podpisanie stosownej pisemnej umowy powierzenia danych zawartej pomiędzy ADO a podmiotem, któremu powierzono przetwarzanie danych osobowych (dalej podmiotem przetwarzającym).
6. Umowa, o której mowa w ust. 5, może być integralną częścią umowy o świadczenie usług lub umowy o realizację zadania wykonywanego na rzecz GDOŚ.
7. Umowy powierzenia danych osobowych lub umowy, których realizacja wymaga powierzenia danych osobowych wykonawcy, podlegają rejestracji w Rejestrze Umów Powierzenia.
8. Jeżeli podmiot przetwarzający zamierza, w ramach realizacji zadań na rzecz GDOŚ, korzystać z podwykonawców i będzie to wiązało się z koniecznością podpowierzenia (przekazania) im powierzonych przez GDOŚ danych osobowych, zobowiązany jest, najpóźniej w dniu podpisania umowy powierzenia danych osobowych przedłożyć listę podmiotów, którym zamierza podpowierzyć dane.
9. Podmiot przetwarzający jest zobowiązany do aktualizacji listy podwykonawców, którym zamierza podpowierzyć dane osobowe przez cały okres realizacji umowy zawartej z GDOŚ.
10. Podmiot przetwarzający jest zobowiązany do poinformowania ADO o zmianach na liście podmiotów, którym zamierzał podpowierzyć dane osobowe, na 14 dni przed ich faktycznym podpowierzeniem.
11. ADO ma prawo, wyrazić sprzeciw co do dalszego podpowierzenia w przypadku gdy :
    1) podwykonawca nie gwarantuje odpowiedniego poziomu bezpieczeństwa danych osobowych;
    2) wobec podwykonawcy Prezes Urzędu Ochrony Danych Osobowych prowadzi lub prowadził postępowanie o naruszenie zasad bezpieczeństwa danych osobowych;

3) podwykonawca, przy realizacji innej umowy lub zadania, nie dochował należytej staranności w zapewnieniu odpowiedniego poziomu bezpieczeństwa danych osobowych.

12. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec ADO za wywiązanie się swoich podwykonawców z obowiązków dotyczących ochrony danych osobowych.
13. ADO ma prawo do kontroli sposobu zabezpieczenia i przetwarzania powierzonych danych osobowych.
14. Kontrolę, o której mowa w ust. 13, mogą prowadzić wyznaczeni pracownicy GDOŚ lub upoważniony podmiot zewnętrzny.
15. Po kontroli, o której mowa w ust. 13, ADO ma prawo wydać podmiotowi przetwarzającemu zalecenia i wytyczne co do sposobu zabezpieczenia i przetwarzania powierzonych danych osobowych.
16. W celu realizacji wspólnych zadań oraz celów przetwarzania danych przez co najmniej dwóch odrębnych administratorów danych osobowych, mogą oni uzgodnić sposób przetwarzania danych oraz zasady współadministrowania danymi osobowymi.
17. Uzgodnienia, o których mowa w ust. 16, co do sposobu przetwarzania, zakresu odpowiedzialności oraz obowiązków wynikających z przepisów RODO zawiera się w umowie lub innym instrumencie prawnym, np. porozumieniu o współpracy („umowa o współadministrowaniu).
18. W umowie o współadministrowaniu danymi osobowymi wskazuje i określa się w szczególności:
    1) zakres odpowiedzialności poszczególnych współadministratorów przy realizacji praw osób fizycznych, których dane dotyczą;
    2) sposób realizacji obowiązków informacyjnych wynikających z art 13 i 14 RODO;
    3) punkt kontaktowy dla osób fizycznych, których dane osobowe są współadministrowane.
19. Najważniejsze uzgodnienia dotyczące zasad współadministrowania danymi osobowymi udostępnia się podmiotom, których dane są współadministrowane. Udostępnienie uzgodnień, o których mowa w zdaniu poprzednim, można zrealizować poprzez zamieszczenie informacji w treści projektu, klauzuli informacyjnej lub np. w materiałach informacyjnych dotyczących przedsięwzięcia.
20. Osobom, których dane dotyczą, przekazuje się informacje, o których mowa w art. 13 i 14 RODO, oraz podział i zakres odpowiedzialności każdego ze współadministratorów. W przekazanej informacji można wskazać jeden punkt kontaktowy dla osób, których dane dotyczą.
21. Niezależnie od uzgodnień w zakresie wspólnego administrowania danymi osobowymi dokonanych przez współadministratorów danych, osoba fizyczna, której dane dotyczą, może realizować prawa przysługujące jej na podstawie RODO niezależnie od każdego z administratorów.

## § 7. Realizacja praw osób, których dane dotyczą

1. Osoba fizyczna, której dotyczą dane, ma prawo do uzyskania od ADO potwierdzenia czy przetwarza on jej dane osobowe, a jeśli przetwarzanie ma miejsce, ma prawo do żądania podania informacji o:
    1) celu przetwarzania;
    2) kategorii przetwarzanych danych osobowych;
    3) informacji o odbiorcach danych osobowych;
    4) informacji, czy jej dane zostały przekazane do państwa trzeciego lub organizacji międzynarodowej;
    5) informacji o planowanym czasie przetwarzania jej danych oraz, gdy jest to możliwe, informacji o kryteriach ustalania tego czasu;
    6) źródle pochodzenia danych, o ile nie pochodzą one bezpośrednio od osoby fizycznej;

7) przysługującym prawie złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

2. Osoba, której dane dotyczą, ma również prawo do uzyskania kopii przetwarzanych danych. Prawo to może być zrealizowane, o ile realizacja tego prawa nie będzie naruszać praw i wolności osób trzecich.
3. Osoba, której dane dotyczą, ma prawo żądać od ADO niezwłocznego sprostowania, poprawienia lub, jeśli jest to niezbędne do realizacji celów przetwarzania, uzupełnienia jej danych osobowych.
4. Osoba fizyczna, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych. ADO ma obowiązek realizacji takiego żądania, jeżeli zachodzi jedna z następujących okoliczności:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   3) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
   4) dane osobowe były przetwarzane niezgodnie z prawem;
   5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega ADO.

   Jeżeli dane osobowe zostały upublicznione (opublikowane), ADO ma obowiązek je usunąć, a także, biorąc pod uwagę koszty i możliwości techniczne, ma obowiązek poinformować innych administratorów danych przetwarzających te dane, że osoba, której dane dotyczą, żąda usunięcia kopii danych ich replikacji oraz wszelkich łączy do tych danych.
5. Prawa, o których mowa w ust. 4, nie będą realizowane w przypadku gdy przetwarzanie danych jest niezbędne do:
   1) realizacji prawa do wolności wypowiedzi i informacji;
   2) wywiązania się z obowiązku prawnego ciążącego na ADO;
   3) wykonania zadania realizowanego w interesie publicznym lub w związku ze sprawowaniem władzy publicznej;
   4) realizacji interesu publicznego w dziedzinie zdrowia publicznego, w szczególności profilaktyki zdrowotnej lub medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia, ochrony przed poważnymi transgranicznymi zagrożeniami zdrowotnymi;
   5) celów archiwalnych, do celów badań naukowych lub historycznych;
   6) celów statystycznych;
   7) do ustalenia, dochodzenia lub obrony roszczeń.
6. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych. Prawo to może być zrealizowane jeżeli :
   1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych. Przetwarzanie ogranicza się na okres pozwalający ADO sprawdzić prawidłowość tych danych;
   2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

3) danych osobowych nie są już niezbędne do realizacji celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania, na mocy art. 21 ust. 1 RODO. Przetwarzanie ogranicza się do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora Danych Osobowych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli przetwarzanie danych zostało ograniczone, to takie dane osobowe można przetwarzać wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Powyższe ograniczenia nie dotyczą przechowywania danych. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, która złożyła żądanie ograniczenia przetwarzania jej danych.

7. ADO ma obowiązek poinformować o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie realizacją wniosków osób fizycznych, o których mowa w ust. 3 i 4, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Jeżeli osoba, której dane zostały sprostowane, usunięte lub których przetwarzanie zostało ograniczone, złoży takie żądanie, ADO przekazuje tej osobie informacje o odbiorcach tych danych.

8. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi, jeżeli łącznie spełnione są poniższe przesłanki:

   1) przetwarzanie odbywa się na podstawie zgody;

   2) przetwarzanie odbywa się na podstawie umowy;

   3) przetwarzanie odbywa się w sposób zautomatyzowany.

   Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, aby dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

   Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO.

9. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, które odbywa się :

   1) w związku z wykonywaniem zadania realizowanego w interesie publicznym lub w związku ze sprawowaniem władzy publicznej;

   2) w związku z uzasadnionym interesem prawnym ADO.

10. W sytuacji, o której mowa w ust. 9, ADO nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

11. Realizacja praw, o których mowa w niniejszym paragrafie, odbywa się na pisemny wniosek osoby, której dane dotyczą.

12. Wniosek, o którym mowa w ust. 11, może być złożony:

   1) w formie tradycyjnej, w kancelarii ogólnej GDOŚ;

   2) w postaci korespondencji elektronicznej, poprzez elektroniczne formy komunikacji (e-PUAP, adres poczty e-mail).

13. Wnioski o realizację praw, o których mowa w niniejszym paragrafie, muszą zawierać informację umożliwiające wyszukanie danych osoby fizycznej w bazach danych GDOŚ oraz muszą umożliwiać weryfikację jej tożsamości. Wniosek musi zawierać dane kontaktowe do osoby składającej żądanie dotyczące danych osobowych.
14. Warunkiem realizacji wniosków o realizację praw osób fizycznych jest potwierdzenie uprawnień i tożsamości wnioskodawcy. Potwierdzenie uprawnień i tożsamości może być zrealizowane:
    1) w przypadku złożenia wniosku w formie, o której mowa w ust. 12 pkt 1 – poprzez weryfikację dokumentu tożsamości wnioskodawcy lub poprzez weryfikację zgodności dodatkowych danych osobowych podanych we wniosku;
    2) w przypadku złożenia wniosku w formie, o której mowa w ust. 12 pkt 2 – poprzez podpisanie wniosku z użyciem podpisu kwalifikowanego lub profilu zaufanego.
15. Realizacja wniosków, o których mowa w ust. 12, może nastąpić jedynie po uzyskaniu opinii IOD lub jego Zastępcy.
16. Wnioski o realizację praw osób fizycznych podlegają rejestracji w Rejestrze Zapytań i Wniosków. Rejestr prowadzi Przedstawiciel Administratora Danych Osobowych. Rejestr może być prowadzony w formie elektronicznej lub papierowej. Wzór Rejestru określa załącznik nr 5 do Polityki Przetwarzania Danych Osobowych.
17. Przy pierwszym kontakcie z osobą fizyczną, której dane dotyczą, pracownicy GDOŚ, osoby realizujące zadania na rzecz GDOŚ na podstawie umowy cywilnoprawnej oraz stażyści i wolontariusze są zobowiązani umożliwić osobie fizycznej, której dane dotyczą, zapoznanie się z informacjami, o których mowa w art. 13 RODO.
18. Informacje, o których mowa w ust. 17. można opracować w postaci klauzuli informacyjnej zawierającej:
    1) nazwę i dane kontaktowe Administratora Danych Osobowych;
    2) dane kontaktowe Inspektora Ochrony Danych;
    3) cel przetwarzania danych osobowych;
    4) podstawę prawną przetwarzania;
    5) informacje o odbiorcach lub kategoriach odbiorców (o ile istnieją);
    6) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (o ile ma to zastosowanie);
    7) możliwości uzyskania kopii danych lub miejscu ich udostepnienia;
    8) okres, przez który dane osobowe będą przetwarzane, lub kryteria ustalenia tego okresu;
    9) informacji o prawie dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie wniesienia sprzeciwu wobec przetwarzania;
    10) jeżeli przetwarzanie danych odbywa się na podstawie zgody (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO) – informację o prawie cofnięcia zgody w dowolnym momencie;
    11) informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
    12) informacje czy podanie danych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są konsekwencje niepodania danych;
    13) informacje o zautomatyzowanym podejmowaniu decyzji w tym profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.

19. Informacji, o których mowa w ust. 18, nie przekazuje się, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami.
20. W przypadku pozyskania danych osobowych osoby fizycznej z innego źródła niż od niej samej, pracownicy GDOŚ, osoby realizujące zadania na rzecz GDOŚ na podstawie umowy cywilnoprawnej oraz stażyści i wolontariusze, są zobowiązani, w imieniu ADO, umożliwić osobie, której dane dotyczą, zapoznanie się z informacjami, o których mowa w art. 14 RODO.
21. Informacje, o których mowa w ust. 20, można opracować w postaci klauzuli informacyjnej zawierającej informacje, o których mowa w ust. 18, oraz uzupełnionej o niżej wymienione informacje:
    1) kategorię odnośnych danych osobowych;
    2) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie, czy pochodzą ze źródeł publicznie dostępnych;
22. Informacje, o których mowa w ust. 17 i 20, przekazuje się osobie, której dane dotyczą :
    1) w rozsądnym terminie po uzyskaniu danych osobowych, nie później jednak niż ciągu miesiąca od ich pozyskania;
    2) jeżeli dane mają być wykorzystane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszym kontakcie z ta osobą;
    3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
23. Informacji, o których mowa w ust. 17 i 20, nie przekazuje się, jeżeli:
    1) osoba, której dane dotyczą dysponuje już tymi informacjami;
    2) udzielenie takich informacji byłoby niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku zgodnie z art. 14 ust. 5 lit. b RODO;
    3) pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane prawem Unii lub prawem krajowym;
    4) dane osobowe musza zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej lub ustawowym obowiązkiem zachowania tajemnicy
24. Klauzule informacyjne publikuje się w Biuletynie Informacji Publicznej oraz na stronie internetowej GDOŚ.
25. Informacje, o których mowa w ust. 17 i 20, powinny łatwo dostępne z pozycji menu głównego strony internetowej GDOŚ.
26. Informacje, o których mowa w ust. 17 i 20, mogą być umieszczane jako dodatkowy stały element umów, wzorów dokumentów, druków oraz wniosków.
27. Treść informacji, o których mowa w ust. 17 i 20, pracownicy GDOŚ, osoby realizujące zadania na rzecz GDOŚ na podstawie umowy cywilnoprawnej oraz stażyści i wolontariusze mogą konsultować z IOD lub jego Zastępcą.

## § 8. Podstawowe zasady bezpieczeństwa przy przetwarzaniu danych osobowych

1. Za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialne są wszystkie osoby upoważnione do przetwarzania danych osobowych w GDOŚ. W celu ochrony danych osoby upoważnione do przetwarzania danych osobowych podczas przetwarzania danych osobowych w formie tradycyjnej (papierowej) winny uwzględniać m.in. następujące zasady:
    1) chronić dane osobowe przed nieuprawnionym udostępnieniem, przechwyceniem, kopiowaniem, modyfikacją lub zniszczeniem;

2) unikać pozostawiania informacji zawierających dane osobowe przy lub w urządzeniach drukujących oraz miejscach i przestrzeniach biurowych, do których mogą mieć dostęp osoby nieupoważnione;

3) nie korzystać, w trakcie wykonywania zadań służbowych poza siedzibą GDOŚ, z publicznych punktów usługowych ksero, sprzętu prywatnego lub innych publicznych urządzeń służących do kopiowania dokumentów, jeśli kopiowane dokumenty zawierają dane osobowe;

4) przy kontakcie osobistym z interesantem, stroną postepowania, osobą której dane dotyczą, w celu potwierdzenia tożsamości i uprawnień do uzyskania informacji, należy stosować zasadę weryfikacji rozmówcy poprzez sprawdzenie dokumentu tożsamości ze zdjęciem;

5) udostępnianie dokumentów lub informacji zawierających dane osobowe, realizowane w trybie przepisów ustawy o dostępie do informacji publicznej lub ustawy o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko, może odbywać się jedynie po anonimizacji danych osób fizycznych, chyba że z przepisów szczególnych regulujących udostępnianie tego rodzaju informacji wynika wyraźnie konieczność udostępnienia konkretnych danych osobowych.

2. Szczegółowe zasady dotyczące zabezpieczenia dokumentów w formie tradycyjnej (papierowej) znajdują się w Regulaminie Bezpieczeństwa Informacji GDOŚ, stanowiącym odrębny dokument.

3. W celu ochrony danych osoby upoważnione do przetwarzania danych osobowych podczas przetwarzania danych osobowych z użyciem sprzętu i oprogramowania informatycznego winny uwzględniać zasady wskazane w Regulaminie Bezpieczeństwa Informacji w GDOŚ.

4. Osoby upoważnione zobowiązane są do przestrzegania zasady czystego biurka i czystego ekranu, o których mowa w Regulaminie Bezpieczeństwa Informacji GDOŚ.

5. Każdy nośnik pamięci wydany uprawnionym użytkownikom systemu teleinformatycznego GDOŚ, przed jego wydaniem do użytkowania, jest rejestrowany w Rejestrze Nośników Danych przez pracowników Zespołu ds. informatyki. Wzór Rejestru określa załącznik nr 4 do Polityki Przetwarzania Danych Osobowych:

   1) Rejestr Nośników Danych może być prowadzony w przy wykorzystaniu oprogramowania do zarządzania zasobami informatycznymi w organizacji;

   2) użytkownik zobowiązany jest okresowo dokonać sprawdzenia przenośnego nośnika informacji pod kątem ewentualnego zainfekowania złośliwym oprogramowaniem.

## § 9. Procedura postępowania w przypadku wystąpienia naruszenia bezpieczeństwa danych osobowych

### §1

1. Każdy pracownik, osoba fizyczna realizująca zadania na podstawie umowy cywilnoprawnej, stażysta oraz wolontariusz wykonujący zadania na rzecz GDOŚ jest odpowiedzialny za bezpieczeństwo informacji i danych osobowych przetwarzanych w związku realizacją ustawowych zadań GDOŚ.

2. Właściwy poziom bezpieczeństwa uzależniony jest od stałego nadzoru nad bezpieczeństwem, reagowania na incydenty związane z bezpieczeństwem, poufnością i dostępnością danych.

3. Osoby upoważnione do przetwarzania danych osobowych oraz pozostali pracownicy GDOŚ zobowiązani są do zgłaszania bezpośrednim przełożonym wszystkich zdarzeń, zaobserwowanych luk w systemie bezpieczeństwa oraz zagrożeń związanych z bezpieczeństwem danych osobowych.

4. Incydenty związane z bezpieczeństwem i ochroną danych osobowych, poza zgłoszeniem do bezpośredniego przełożonego, podlegają obowiązkowemu zgłoszeniu IOD lub jego Zastępcy. Zgłoszenia incydentów i zagrożeń dotyczących bezpieczeństwa danych osobowych dokonuje się na adres e-mail:

inspektor.ochrony.danych@gdos.gov.pl. Powiadomienie może nastąpić także w formie zgłoszenia osobistego oraz telefonicznego.

5. Jeżeli zgłoszenie incydentu lub zagrożenia bezpieczeństwa danych osobowych dotyczy danych przetwarzanych przy wykorzystaniu zasobów informatycznych GDOŚ, dodatkowo zgłoszenie wysyła się na adres e-mail: incydent@gdos.gov.pl.
6. Zgłoszenie incydentu związanego z bezpieczeństwem danych osobowych dokonuje się zgodnie z postanowieniami zawartymi w **Procedurze zarządzania incydentami bezpieczeństwa informacji, w tym danych osobowych w GDOŚ**, która stanowi odrębny dokument.
7. Jeżeli zgłoszenie naruszenia zasad bezpieczeństwa ochrony danych osobowych stwarza wysokie ryzyko dla osób fizycznych, których dane dotyczą, ADO zobowiązany jest do zawiadomienia organu nadzorczego ds. ochrony danych osobowych. O ile to możliwe, zawiadomienia dokonuje się w terminie 72 godzin od dnia zgłoszenia naruszenia (zdarzenia). Zawiadomienie, o którym mowa wyżej, dokonuje się w formie i na zasadach określonych w art 33 RODO.
8. Treść zawiadomienia, o którym mowa w ust. 7, ADO konsultuje się z IOD lub jego Zastępcą.
9. W przypadku naruszenia zasad bezpieczeństwa informacji i danych osobowych, skutkującego wysokim ryzykiem naruszenia praw i wolności osób fizycznych, obowiązkiem ADO jest zawiadomienie osób, których dane dotyczą, o zaistniałym zdarzeniu i poinformowanie o związanym z tym zdarzeniem ryzykiem dla bezpieczeństwa ich danych.

   Wysokie ryzyko naruszenia praw lub wolności osób fizycznych należy rozumieć w szczególności jako ujawnienie, zniszczenie lub kradzież danych i informacji:

   1) o których mowa w art 9 i 10 RODO – np. dane o stanie zdrowia, o przynależności do związków zawodowych, o wyrokach skazujących lub czynach zabronionych;
   2) umożliwiając kradzież tożsamości osoby fizycznej – np. dane identyfikacyjne, w tym numer ewidencyjny PESEL, numer dokumentu tożsamości itp.;
   3) umożliwiających zaciągnięcie zobowiązań finansowych w imieniu osoby fizycznej, np. dane identyfikacyjne, w tym numer ewidencyjny PESEL, numer dokumentu tożsamości itp.
10. Zawiadomienie, o którym mowa w ust. 9, powinno zawierać elementy, o których mowa w art 33 ust. 3 lit. b, c i d RODO. Zawiadomienia dokonuje się bez zbędnej zwłoki i można tego dokonać poprzez:

    1) wysłanie indywidualnych zawiadomień do osób, których dane zostały zagrożone (drogą elektroniczną, korespondencją pocztową, za potwierdzeniem odbioru);
    2) ogłoszenia prasowe lub publikacja na stronach internetowych, jeśli koszty zawiadomień indywidualnych były niewspółmiernie wysokie do założonego celu.

## § 10. Kontrola i nadzór nad przetwarzaniem danych i stanu ich zabezpieczania

1. Wszystkie osoby zatrudnione w GDOŚ są odpowiedzialne za bezpieczeństwo przetwarzanych danych osobowych.
2. Przed przystąpieniem do pracy pracownicy sprawdzają:

   1) stan zastosowanych zabezpieczeń, w tym w szczególności ewentualne ślady ingerencji lub prób ingerencji w stan zabezpieczeń przez osoby trzecie, oraz stan sprzętu komputerowego, który powinien odpowiadać stanowi, w jakim go pozostawili kończąc pracę;
   2) kompletność powierzonych im dokumentów i innego wyposażenia.

3. W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, pracownik, który stwierdził nieprawidłowość, natychmiast powiadamia o tym swojego bezpośredniego przełożonego i Dyrektora Biura Dyrektora Generalnego GDOŚ. Powiadomienie dokonane w formie ustnej wymaga potwierdzenia w formie pisemnej lub dokumentowej. Jeśli sytuacja tego wymaga, o nieprawidłowościach powiadamia się również Administratora Bezpieczeństwa Teleinformatycznego oraz IOD lub jego Zastępcę.
4. Dyrektorzy Departamentów lub Biur sprawują stały nadzór nad sposobem przetwarzania danych osobowych ich zabezpieczeniem i przestrzeganiem zasad bezpieczeństwa przez podległych pracowników.
5. Nadzór, kontrolę i koordynację działań dotyczących ochrony danych osobowych przetwarzanych w GDOŚ w imieniu Administratora Danych Osobowych sprawuje Zespół do spraw Zarządzania Bezpieczeństwem Informacji, o którym mowa w Polityce Bezpieczeństwa Informacji, stanowiącej odrębny dokument.
6. W ramach prowadzonego nadzoru i kontroli sposobu przetwarzania danych osobowych IOD, samodzielnie lub w porozumieniu z Administratorem Bezpieczeństwa Teleinformatycznego, audytorem wewnętrznym lub inną osobą wyznaczoną przez ADO, przeprowadza weryfikację, kontrolę i audyty sposobu przetwarzania danych osobowych oraz przestrzegania zasad bezpieczeństwa przetwarzania danych.
7. W ramach czynności kontrolnych prowadzonych przez IOD ma on prawo do:
    1) zapoznania się z treścią dokumentów;
    2) zbieranie ustnych i pisemnych wyjaśnień od osób zatrudnionych w GDOŚ;
    3) dostępu do stref przetwarzania danych, pomieszczeń biurowych i archiwum, także pod nieobecność pracowników tam zatrudnionych;
    4) przeprowadzania oględzin miejsc przetwarzania danych osobowych;
    5) wykonania kopii dokumentów;
    6) sporządzenia dokumentacji fotograficznej;
    7) wglądu w systemy teleinformatyczne służące do przetwarzania danych osobowych;
    8) przeglądania zawartości służbowych kont poczty elektronicznej;
    9) sprawdzenia zawartości i sposobów zabezpieczenia nośników danych.
8. IOD na 14 dni przed rozpoczęciem czynności kontrolnych zawiadamia Dyrektora Generalnego GDOŚ o zakresie i terminie kontroli.
9. Zawiadomienia nie przekazuje się w przypadku sprawdzenia doraźnego, jeśli niezwłoczne rozpoczęcie czynności jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji czy naruszenie miało miejsce oraz w przypadku sprawdzenia, o którego dokonanie zwrócił się organ nadzorczy ds. ochrony danych osobowych, jeśli na zawiadomienie nie pozwala termin wyznaczony przez ten organ.
10. Po uzgodnieniu z Dyrektorem Generalnym GDOŚ IOD może wystąpić o wydanie opinii przez osobę posiadającą wiedzę specjalistyczną, niedotyczącą przepisów o ochronie danych osobowych, o ile taka opinia jest niezbędna do zapewnienia prawidłowości przeprowadzanego procesu kontroli lub audytu.
11. Z przeprowadzonych czynności kontrolnych IOD sporządza sprawozdanie dla ADO.
12. Kopię sprawozdania IOD przekazuje do Zespołu do spraw Zarządzania Bezpieczeństwem Informacji.
13. Dyrektorzy Departamentów lub Biur są zobowiązani do zapewnienia, że wszystkie procedury bezpieczeństwa obszaru, za który są odpowiedzialni, wykonywane są prawidłowo, tak aby osiągnąć zgodność z niniejszą Polityką oraz innymi dokumentami obowiązującymi w GDOŚ dotyczącymi bezpieczeństwa informacji.

## § 11. Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO.

## § 12. Załączniki

Załącznikami do niniejszej procedury są:

1) Załącznik nr 1 – Wzór Rejestru Czynności Przetwarzania.
2) Załącznik nr 2 – Wzór Rejestru Kategorii Czynności Przetwarzania.
3) Załącznik nr 3 – Wzór Rejestru Umów Powierzenia.
4) Załącznik nr 4 – Wzór Rejestru Nośników Danych.
5) Załącznik nr 5 – Wzór Rejestru Zapytań i Wniosków.
6) Załącznik nr 6 – Wzór Rejestru Osób Upoważnionych do Przetwarzania Danych Osobowych.
7) Załącznik nr 7 – Wzór upoważnienia do przetwarzania danych osobowych.
8) Załącznik nr 8 – Wzór oświadczenia o zachowaniu poufności.
9) Załącznik nr 9 – Wzór wniosku o nadanie uprawnień i upoważnienia do przetwarzania danych osobowych.
10) Załącznik nr 10 – Wzór oświadczenia wykonawcy.

# Załącznik nr 1 - Wzór Rejestru Czynności Przetwarzania

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| l.p. | Czynność Przetwarzania | Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeśli jest to możliwe) | Administrator | | | | | |
| | | | Nazwa i dane kontaktowe administratora | Nazwa i dane kontaktowe współadministratora (jeśli dotyczy) | Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono) | Inspektor ochrony danych (jeśli wyznaczono) | Lokalizacja przetwarzanych danych osobowych | Sposoby ochrony przetwarzanych danych osobowych, zastosowane zabezpieczenia |
| 1 | Art. 30 ust. 1 | Art. 30 ust. 1 lit. g art. 32 ust. 1 | Art. 30 ust. 1 lit. a | | | | | |
| 2 | **PRZYKŁAD** rejestr skarg i wniosków składanych do GDOŚ | dostęp do danych otrzymują osoby wskazane przez administratora | Generalny Dyrektor Ochrony Środowiska ul. Wawelska 52/54 00-0922 Warszawa | nie dotyczy | nie dotyczy | wypełnia Inspektor Ochrony Danych | Warszawa, ul. Wawelska 52/54 (dokumentacja papierowa; dokumentacja elektroniczna - zgodnie z rozwiązaniami BDG-WI) | dokumenty przechowywane w zamykanych szafach, pliki komputerowe dostępne dla osób posiadających upoważnienie |
| 3 | | | | | | | | |

**część 1z3**

| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|
| Czas trwania przetwarzania danych osobowych | Cel przetwarzania | Kategorie osób | Kategorie danych | Wskazanie szczególnej podstawy prawnej przetwarzania danych osobowych – art. 6 RODO | Wskazanie szczególnej podstawy prawnej przetwarzania danych osobowych – art. 9 RODO | Źródło przetwarzanych danych osobowych | Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane |
| art. 30 ust. 1 lit. f) | art. 30 ust. 1 lit. b) | art. 30 ust. 1 litc) | art. 30 ust. 1 lit. c) | art. 6 ust. 1 | art. 9 ust. 2 | art. 6 i 9 | Art. 30 ust. 2 lit. c |
| zgodnie z obowiązującymi przepisami archiwizacyjnymi | rozpatrywanie składanych skarg wniosków i petycji | osoby fizyczne | np.: (dane kontaktowe) ulica, adres e-mail, telefon | wykonanie zadania w interesie publicznym i w zakresie sprawowania władzy publicznej | | wykonanie zadania w interesie publicznym i w zakresie sprawowania władzy publicznej | |
| | | | | | | | |

**(część 2z3)**

| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|
| Sposoby ochrony danych osobowych przekazanych do państw trzecich lub organizacji międzynarodowych, dokumentacja odpowiednich zabezpieczeń | Zastosowane techniczne środki ochrony danych osobowych przekazanych do państw trzecich lub organizacji międzynarodowych, dokumentacja odpowiednich zabezpieczeń | Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi | Podprzetwarzający (podwykonawca) - jeśli dotyczy | | Czy dotychczas miało miejsce naruszenie zasad ochrony danych osobowych - włamanie do przechowywanych danych osobowych - jeśli tak, to kiedy i jakie | Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców z państw trzecich lub organizacji międzynarodowych |
| | | | Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy) | Kategorie podpowierzonych przetwarzań | | |
| | | Art. 30 ust. 2 lit. c | | | | Art.. 30 ust. 1 pkt d |
| | | | | | nie wystąpiło naruszenie zasad ochrony danych osobowych | |
| | | | | | | |

**(część 3z3)**

Załącznik nr 2 - Wzór Rejestru Kategorii Czynności Przetwarzania.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LP. | Kategorie przetwarzań | Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe) | Administrator | | | | Czas trwania przetwarzania | Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane | Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi | Podprzetwarzający (podwykonawca) - jeśli dotyczy | |
| | | | Nazwa i dane kontaktowe administratora | Nazwa i dane kontaktowe współadministratora (jeśli dotyczy) | Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono) | Inspektor ochrony danych administratora (jeśli powołano) | | | | Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy) | Kategorie podpowierzonych przetwarzań |
| | Art. 30 ust. 2 lit. b | Art. 30 ust. 2 lit. d, art. 32 ust. 1 | Art. 30 ust. 2 lit. a | | | | | Art. 30 ust. 2 lit. c | Art. 30 ust. 2 lit. c | | |
| 1 | PRZYKŁAD: Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia rekrutacji pracowników w środowisku sprzętowo-programowym wynajętym przez przetwarzającego | • Kontrola dostępu do infrastruktury, aplikacji i baz danych.<br>• Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funkcjonalności, konserwacyjne, naprawcze).<br>• Szyfrowana transmisja danych. | Agencja Pracy XYZ<br>ul. Przykładowa 35/3<br>00-950 Warszawa<br><br>kontakt@przedsiebiorstwrekrutacyjnea.pl<br><br>tel.: 133 456 888 | Agencja pracy ABC<br>ul. Przykladowa 5/2<br>00-950 Warszawa<br>kontakt@agencjaabc.pl<br>tel.: 133 456 888 | Jan Headhunter<br>JanH@agencjaabc.pl<br>tel.: 444 565 321 | wypełnia Inspektor Ochrony Danych | 29 marca 2019 r. | Nie dotyczy | Nie dotyczy | G.H.C. Centre de données exemplaire<br>ul. Exemple De Rue 3/4<br>13012 Marsylia, Francja<br>info@centrededonneesexample.fr | Przechowywanie, udostępnianie, utrwalanie i usuwanie danych w ramach udostępnianiej mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej. |

Załącznik nr 3 - Wzór Rejestru Umów Powierzenia.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| **l.p.** | **Nr umowy (dokumentu)** | **Z kim podpisano umowę (nazwa, adres)** | **Data podpisania umowy** | **Okres obowiązywania umowy (data zakończenia)** | **Biuro/Departament podpisujący umowę** | **Zakres powierzonych danych osobowych** | **Nazwa systemu/bazy danych/programu** | **Po zakończeniu umowy dane osobowe są: (zwracane, niszczone)** | **Uwagi** |
| **1** | **przykład:** umowa 2/BP/GDOŚ | Pentacomp Syst.Inf. S.A., Warszawa, ul. Al..Jerozolimskie 179 | 1.01.2020 | 31.12.2021 | BP | dane osobowe przetwarzane w ramach programu "XYZ" | np. FT-Kadry | | |
| **2** | **przykład:** umowa 12/BP/GDOŚ | AAABBBCCC | 2.02.2020 | 31.12.2020 | BP | imię i nazwisko, nr. telefonu, e-mail, adres IP, adres zamieszkania, płeć, nazwisko, nazwisko rodowe, PESEL, miejsce urodzenia, adres zameldowania, obywatelstwo, imię ojca, imię matki, rodzaj dokumentu tożsamości i jego numer | | | |
| **3** | | | | | | | | | |

Załącznik nr 4 - Wzór Rejestru Nośników Danych.

# REJESTR NOŚNIKÓW DANYCH

| Lp. | nr ewid. | rodzaj nośnika/typ komputera | typ /model/nr seryjny | wielkość / pojemność | data wydania do użytku | wydano (imię nazwisko pracownika) | podpis pracownika | data zwrotu / podpis prac. Zespół ds. informatyki | adnotacja o zniszczeniu, lub nr pisma za którym przesłano nośnik |
|---|---|---|---|---|---|---|---|---|---|
| 1. | 001 | HDD/i5-4460/8GB/Logic/ GT730<br>**PRZYKŁAD** | ToshibaHDWD110 /<br>SN:X6LS4RZFS | 1TB | 1.12.2021 | Kowalski Jan | | Nie dotyczy | odesłano do MKiŚ - pismo nr 2022/001/GDOŚ/2022 |
| 2. | 002 | HDD/i32120/8GB/ W7Pro<br>**PRZYKŁAD** | WD5000/SN: WD-WCC1U0032349 | 500MB | 22.01,2022 | Nowak Jerzy | | 22.02.2021 - Marek Iksiński | zniszczono 25.02.2021 - Marek Iksiński - spec IT |
| 3. | 003 | HDD/E6500/500GB/3GB/ W7<br>**PRZYKŁAD** | WD500/<br>SN:WD-WCAV9D255986 | 500MB | 13.02.2022 | Anna Kowalska | | Nie dotyczy | |

Załącznik nr 5 – Wzór Rejestru Zapytań i Wniosków

| REJESTR ZAPYTAŃ i WNIOSKÓW | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Lp.** | **data wpływu** | **numer ewidencyjny z dziennika korespondencji** | **podmiot danych/imię nazwisko wnioskodawcy** | **podstawa prawna i opis żądania lub wniosku** | **opinia IOD** | **sposób realizacji wniosku lub żadania** | **data realizacji wniosku lub żadania** | **numer pisma zawiadamiającego o realizacji lub odmowie realizacji wniosku** | **uwagi** |
| **1** | 22.01.2021 | GDOŚ/345/01/2021 **Przykład** | KOWALSKI JAN | art. 15 RODO - żądanie potwierdzenia przetwarzania danych | żądanie uzasadnione i wymaga udzielenia odpowiedzi zawierającej elementy o których owa w art. 15 ust 1 RODO | Zrealizowano - weryfikacja baz danych, pod kątem wyszukania rekordów z danymi wnioskodawcy | 30.01.2021 | GDOŚ/543/01/2021 | |
| **2** | 13.02.2022 | GDOŚ/05/02/2022 **Przykład** | NOWAK JAN | art 17 RODO- żądanie usunięcia danych | przepisy ustawy o zasobach archiwalnych nie zezwalają na realizację żądania | nie zrealizowano | wniosku nie zrealizowano | GDOŚ/105/02/2022 | |
| **3** | | | | | | | | | |

Załącznik nr 6 – Wzór Rejestru Osób Upoważnionych do Przetwarzania Danych Osobowych

# REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

| Lp. | numer upoważnienia | nazwisko | imię | stanowisko służbowe | departament/komurka organizacyjna | data wydania upoważnienia | data ważności upoważnienia | login nadany przez IT | zakres upoważnienia | data szkolenia z zakresu RODO |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | KOWALSKI | Jan | specjalista | kadry | 22.01.2022 | do odwołania | jankowalski | 1.ewidencja pracowników; 2.rozliczenia z ZUS; lista płac; 3. Urlopy | 02.02.2022 |
| 2 | 2 | NOWAK | Tomasz | radca prawny | Biuro prawne | 25.03.2022 | 31.12.2022 | tomasznowak | 1. Strony postępowań administracyjnych; | 02.04.2022 |
| 3 | | | | | | | | | | |
| 4 | | | | | | | | | | |

Załącznik nr 7 – Wzór upoważnienia do przetwarzania danych osobowych.

numer upoważnienia …….. Warszawa dnia ……..

# U P O W A Ż N I E N I E

## DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych Osobowych w Generalnej Dyrekcji Ochrony Środowiska w Warszawie, ul. Wawelska 52/54 , 00-922 Warszawa, na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE ( „RODO” ) oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych ( Dz. U. z 2019 r. poz. 1781)

## U P O W A Ż N I A M

| | | |
|---|---|---|
| **Imię i nazwisko upoważnionego pracownika / stanowisko służbowe** | | |
| | | |
| **Zakres danych objętych upoważnieniem** | | |

Osoba upoważniona zobowiązana jest przetwarzać dane osobowe zawarte w w/w zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.
Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Generalnej Dyrekcji Ochrony Środowiska wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Upoważnienie jest ważne do: ……..….
Upoważnienie traci moc w momencie cofnięcia, upływu terminu nadania upoważnienia lub ustania stosunku pracy.
Traci moc upoważnienie do przetwarzania danych osobowych nr ……. z dnia ……. r.

…… ……..

Załącznik nr 8 – Wzór oświadczenia o zachowaniu poufności.

# O Ś W I A D C Z E N I E

1. Zostałam/em zaznajomiona/y z przepisami ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ).
2. Zostałam/em zaznajomiona/y z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE: L z dnia 04.05.2016r . Nr 119/1),zwanym „RODO”
3. Zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w „Regulaminie Bezpieczeństwa Informacji” oraz zobowiązuję się do ich przestrzegania
4. Znana jest mi odpowiedzialność karna za naruszenie przepisów, o których mowa w ust. 1 i 2 i jestem świadomy/a, że naruszenie tych przepisów oraz zasad, o których mowa w ust. 3, może stanowić naruszenie obowiązków pracowniczych.
5. Zobowiązuję się:
    a) zachować w tajemnicy dane osobowe, z którymi zetknęłam się/zetknąłem się lub zetknę się w trakcie wykonywania swoich obowiązków służbowych oraz znane mi sposoby ich zabezpieczenia, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu,
    b) chronić dane osobowe przed dostępem osób nieuprawnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.

Warszawa dnia …… ……

(podpis osoby upoważnionej )

Załącznik nr 9 – Wzór wniosku o nadanie uprawnień i upoważnienia do przetwarzania danych osobowych.

**WNIOSEK O NADANIE/ODEBRANIE/ZMIANĘ UPRAWNIEŃ W SYSTEMACH I ZASOBACH ORAZ O NADANIE/ODEBRANIE/ZMIANĘ UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH**

| **Wniosek w związku:** | |
|---|---|
| • zatrudnieniem nowego pracownika | ☐ *Kliknij lub naciśnij, aby wprowadzić datę.* |
| • ze zmianą w strukturze GDOŚ (przeniesieniem) | ☐ *Kliknij lub naciśnij, aby wprowadzić datę.* |
| • ze zmianą stanowiska służbowego | ☐ *Kliknij lub naciśnij, aby wprowadzić datę.* |
| • objęciem nowej funkcji | ☐ *Kliknij lub naciśnij, aby wprowadzić datę.* |
| • dodaniem dodatkowych uprawnień | ☐ *Kliknij lub naciśnij, aby wprowadzić datę.* |
| • zakończeniem stosunku pracy | ☐ *Kliknij lub naciśnij, aby wprowadzić datę.* |

| **Informacje o pracowniku** | | |
|---|---|---|
| **Nazwisko i imię pracownika** | *WPROWADZIĆ TEKST* | |
| **Komórka organizacyjna** | *Wybierz z listy* | *Wybierz z listy* |
| | **Departament** | **Wydział/Zespół** |
| **Stanowisko służbowe** | *Wybierz z listy stanowisko lub naciśnij tutaj, aby wprowadzić tekst.* | |
| **Dodatkowe funkcje** | *Wybierz z listy* | |
| **Dodatkowe informacje** | *Kliknij lub naciśnij tutaj, aby wprowadzić tekst.* | |

**Lokalizacja:** *Wybierz z listy* **pokój nr** *wpisz piętro/pokój*

**Wnioskuję o** *Wybierz z listy* **podległemu pracownikowi dostępu do następujących systemów/zasobów informatycznych:**

| **Typ/Nazwa systemu** | **Program/Zasoby** |
|---|---|
| **Poczta elektroniczna (skrzynka e-mail)**<br>**– MS Outlook** | ☐ |
| **Dostęp do innych skrzynek e-mail** | *Wskaż adres email* |
| **Dostęp do aliasów – grup** | *Wskaż adres email aliasu* |

| | |
|---|---|
| **dystrybucyjnych** | |
| **Dostęp do dysków wspólnych** | *Podaj nazwę udziału* |
| **QNT** | **Dostęp do modułu:** *Wybierz z listy*<br>**Dodatkowe:** *Wybierz z listy*<br>*Wybierz z listy* |
| **Płatnik** | ☐ |
| **Lex** | ☐ |
| **Inne** | *wprowadzić inne programy.* |

| **System Elektronicznego Zarządzania Dokumentacją** | | |
|---|---|---|
| | Inicjały pracownika w EZD *wprowadź* | |
| Wnioskuję o Wybierz z listy | | |
| Grupy upoważnień | PRZYDZIELONE | ODEBRANE |
| • Domyślna | ☐ | ☐ |
| • Naczelnik Wydziału (kierujący zespołem) | ☐ | ☐ |
| • Dyrektor i Z-ca Departamentu | ☐ | ☐ |
| • Kierownictwo GDOŚ | ☐ | ☐ |
| • Kancelaria | ☐ | ☐ |
| • Sekretariat | ☐ | ☐ |
| • Podpis Kwalifikowany | ☐ | ☐ |
| • Profil Zaufany | ☐ | ☐ |
| • Archiwum | ☐ | ☐ |
| • Zarządzanie zasobami (sala 455/konf) | ☐ | ☐ |
| • Administracja EZD | ☐ | ☐ |
| Inne uprawnienia ☐ | | |
| *Wskaż inne uprawnienia* | | |
| Dostęp do RWA innej komórki org. ☐ | | |
| *Wskaż komórkę organizacyjną/rwa/rok* | | |
| Dostęp do zasobów innej komórki org ☐ | | |

| *Wskaż komórkę organizacyjną/rok i uzasadnienie* |
|---|
| Dostęp do raportów/rejestrów ☐ |
| *Wskaż raporty i rejestry* |

**Konto na które mają zostać przekazane wszystkie niezakończone koszulki w przypadku wniosku o zamknięcie/zawieszenie konta EZD** *Wpisz imię i nazwisko pracownika*

| **WNIOSKOWANY ZAKRES UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH** | | | |
|---|---|---|---|
| **Lp.** | **Zakres danych osobowych**<br>**(nazwa z kolumny 2 Rejestru Czynności Przetwarzania (RCP) – art. 30 ust 1 RODO)** | **Cel przetwarzania**<br>**(nazwa z kolumny 11 Rejestru Czynności Przetwarzania (RCP) – art. 30 ust 1 lit. b) – wypełnić jeśli upoważnienie nie dotyczy całego zakresu danych osobowych z kolumny 2 RCP )** | **Data ważności upoważnienia**<br>**(uzupełnić jeśli umowa o pracę/umowa zlecenie/itp. jest na czas określony, lub upoważnienie dotyczy ograniczonego czasu)** |
| **1** | | | |
| **2** | | | |
| **3** | | | |
| **4** | | | |

| **Akceptacja:** Wpisz imię i nazwisko pracownika akceptującego/przełożonego | |
|---|---|
| **Stanowisko przełożonego/akceptującego:**<br><br>**Data akceptacji przełożonego** Kliknij lub naciśnij, aby wprowadzić datę | |
| Wpisz imię i nazwisko pracownika<br><br>**Akceptacja ADO** | Kliknij lub naciśnij, aby wprowadzić datę.<br><br>**Data** |

Załącznik nr 10 – Wzór oświadczenia wykonawcy.

**Oświadczenie wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO**

Oświadczam, że zapoznałem się z „Klauzulą informacyjną RODO" zawartą w zapytaniu ofertowym pkt. …….

Ponadto oświadczam, że na podstawie art. 14 RODO zapoznałem z „Klauzulą informacyjną RODO" zawartą w zapytaniu ofertowym/zamówieniu publicznym* pkt. …… wszystkie osoby fizyczne, których dane przekazuje zamawiającemu i których dane pośrednio pozyskałem.

…....., dnia …..... …….

podpis osoby uprawnionej

**Oświadczenie wykonawcy w zakresie wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych gwarantujących bezpieczeństwo danych osobowych**

Oświadczam, że w celu zagwarantowania bezpieczeństwa powierzonych danych osobowych, niezbędnych dla realizacji zadania będącego przedmiotem zapytania ofertowego/zamówienia publicznego*, w ……..wprowadzono:

(nazwa oferenta/ wykonawcy )

1. odpowiednie rozwiązania organizacyjne i techniczne gwarantujące bezpieczeństwo danych osobowych - TAK / NIE *
2. personel realizujący zadanie posiada odpowiednie przeszkolenie i upoważnienia z zakresu ochrony danych osobowych - TAK / NIE *
3. rejestr kategorii czynności przetwarzania - TAK /NIE*
4. powołano Inspektora Ochrony Danych Osobowych - TAK / NIE * - który jest dostępny pod adresem email…… ; nr telefonu ……

…....., dnia …..... …….

podpis osoby uprawnionej

*niepotrzebne skreślić

**Załącznik nr 2** do Zarządzenia nr 14 Generalnego Dyrektora Ochrony Środowiska w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska z dnia 17 listopada 2022 r.

# *Regulamin Bezpieczeństwa Informacji Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Generalny Dyrektor Ochrony Środowiska

ANDRZEJ SZWEDA-LEWANDOWSKI

Generalny Dyrektor Ochrony Środowiska……

Generalny Dyrektor Ochrony Środowiska

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Niniejszy dokument definiuje i opisuje najważniejsze zasady bezpieczeństwa informacji dla wszystkich osób mających dostęp do informacji przetwarzanych w Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ". Głównym jego celem jest zwiększanie świadomości w zakresie bezpieczeństwa informacji oraz ochrona przed naruszeniami ich bezpieczeństwa.

## § 2. Zakres

Niniejszy dokument obejmuje zasadami wszystkie osoby mające dostęp do Aktywów Informacyjnych GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszym Regulaminie jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.
2) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;
3) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. NICK, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
4) **Dostępności** – należy przez to rozumieć właściwość bezpieczeństwa aktywa oznaczający dostępność informacji dla osób uprawnionych wtedy, gdy jest to niezbędne dla potrzeb ich przetwarzania, właściwość aktywa do bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
5) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 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), którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.
6) **Integralności** – należy przez to rozumieć atrybut bezpieczeństwa aktywa i zasobu informacyjnego określający jakość informacji w aspekcie kompletności, spójności i wiarygodności danych.

7) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;

8) **Nośniku danych** – należy przez to rozumieć urządzenie, papier lub inny nośnik, na którym zapisuje się i przechowuje informacje.

9) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;

10) **Poufności** – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

11) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);

12) **Przełożonym** – należy przez to rozumieć bezpośredniego zwierzchnika;

13) **Rejestrze nośników danych** – należy przez to rozumieć rejestr prowadzony przez Kierującego zespołem do spraw informatyki lub innego wyznaczonego pracownika zespołu do spraw informatyki, zawierający informacje dotyczące zasobów informatycznych wykorzystywanych jako nośniki danych. Rejestr zawiera zarówno informacje dotyczące nośników danych zainstalowanych w urządzeniach stacjonarnych oraz mobilnych (dyski i pamięć wewnętrzna) jak również pamięci masowych oraz nośników optycznych (pendrive, płyty CD, DVD itp.);

14) **Systemie teleinformatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

15) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ;

16) **Uwierzytelnianiu** – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

## § 4. Odpowiedzialność i uprawnienia

1. Za nadzór nad przestrzeganiem zapisów niniejszego regulaminu odpowiedzialni są:
   1) Dyrektor Generalny GDOŚ;
   2) Pełnomocnik ds. BI;
   3) ABT;
   4) KKO.
2. Zasady wynikające z zapisów niniejszego regulaminu obowiązują wszystkie osoby mające dostęp do informacji przetwarzanych w GDOŚ i są one zobowiązane do ich stosowania, a ich naruszenie może skutkować postępowaniem dyscyplinarnym, cywilnym lub karnym.
3. Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszego Regulaminu został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Podstawowe zasady bezpieczeństwa informacji

1. Każda osoba mająca dostęp do informacji ma obowiązek chronić je przed naruszeniem Poufności, Integralności oraz Dostępności. W szczególności należy chronić informacje przed nieuprawnionym udostępnieniem, przechwyceniem, kopiowaniem, modyfikacją lub zniszczeniem.
2. Informacje należy chronić w swoim miejscu pracy poprzez utrzymywanie uporządkowanego biurka (tzw. polityka czystego biurka) i zamykając poszczególne pomieszczenia i szafy. Dokumenty i Nośniki danych należy przechowywać w zamkniętych obszarach lub szafach biurowych, gdy nie są używane lub po godzinach pracy tak, aby zagwarantować, że nie będzie miała do nich dostępu osoba nieupoważniona.
3. Informacji podlegających ochronie nie wolno umieszczać w miejscach ogólnodostępnych przestrzeni biurowej, aby nie mogły być przypadkowo odczytane przez osoby nieupoważnione.
4. Opuszczając miejsce pracy, użytkownik musi być zawsze wylogowany z systemu operacyjnego (klawisze WIN „+” L na klawiaturze komputera). Należy stosować zasadę czystego ekranu w celu zapewnienia, iż osoby nieuprawnione nie mają możliwości wglądu w treści wyświetlane na monitorze komputera.
5. Chroniony hasłem wygaszacz ekranu powinien być aktywowany automatycznie po 15 minutach braku aktywności na komputerze.
6. Monitor powinien być ustawiony w sposób uniemożliwiający osobom nieupoważnionym na wgląd i dostęp do wyświetlanych informacji.
7. Po zakończeniu pracy należy się wylogować z systemu i wyłączyć komputer.
8. Żadne informacje nie mogą być pozostawione niezabezpieczone w miejscu pracy pod nieobecność osób upoważnionych do dostępu do nich.
9. Wszelkie informacje wykorzystywane w salach konferencyjnych należy usunąć po spotkaniu. Zapisane tablice należy wyczyścić.
10. Wydrukowane dokumenty należy natychmiast zabierać z drukarek i faksów.
11. Wszystkie niepotrzebne dokumenty, notatki lub błędy drukarskie należy zniszczyć przy użyciu niszczarki.
12. Zabrania się korzystania przez kilka osób z jednego identyfikatora w danym systemie/aplikacji. Udostępnianie swoich danych do logowania innym osobom jest zabronione.
13. W przypadku korzystania z dwuskładnikowego Uwierzytelniania (2FA), Nośnik (np. smartfon, token) musi być chroniony przed nieautoryzowanym dostępem – nie może być swobodnie dostępny podczas opuszczania miejsca pracy.
14. W przypadku zaatakowania urządzenia przez złośliwe oprogramowanie (tzw. malware) lub podejrzenia takiego zdarzenia, należy niezwłocznie poinformować pracowników Wydziału Informatyki BDG oraz natychmiast odłączyć urządzenie od sieci komputerowej. **UWAGA! Nie należy wyłączać urządzenia!**
15. Sprzęt i oprogramowanie przekazane przez pracodawcę powinno być wykorzystywane wyłącznie do celów służbowych.
16. Sprzęt służbowy nie może być udostępniany osobom nieupoważnionym.
17. Informacje sklasyfikowane jako Aktywa Informacyjne klasy IV należy oznaczać w wyraźny sposób dopiskiem „DOKUMENTY SZCZEGÓLNIE CHRONIONE”
    1) w przypadku dokumentów papierowych na pierwszej stronie i na okładce (np. segregator, grzbiet);

2) w przypadku dokumentów elektronicznych w nazwie pliku oraz na pierwszej stronie.

**UWAGA! Dokumenty oznaczane są od momentu rozpoczęcia tworzenia informacji.**

18. W zakresie zapewnienia bezpieczeństwa przetwarzanych w GDOŚ Danych osobowych obowiązują zasady opisane w ***Polityce Przetwarzania Danych Osobowych***.

## § 6. Urządzenia mobilne, komunikacja telefoniczna i kontakt osobisty

1. W przypadku korzystania z urządzeń mobilnych, niezależnie od stosowanych odpowiednio zasad wskazanych w § 5, stosuje się poniższe zasady
   1) urządzenia powinny być fizycznie zabezpieczane przed kradzieżą, zwłaszcza w przypadku pozostawiania ich w samochodach i innych środkach transportu, pokojach hotelowych, centrach konferencyjnych i miejscach spotkań;
   2) urządzenia, na których znajdują się ważne, wrażliwe lub krytyczne informacje, nie powinny być pozostawiane bez nadzoru i, o ile to możliwe, powinny być fizycznie zablokowane lub chronione poprzez zastosowanie specjalnych zamków do zabezpieczenia urządzeń
2. W celu zapewnienia bezpieczeństwa informacji wszystkie osoby zobowiązane są do stosowania niżej wymienionych zasad podczas komunikowania się za pomocą środków komunikacji telefonicznej oraz podczas kontaktów osobistych:
   1) korzystając z łączności telefonicznej, przed przekazaniem informacji o charakterze chronionym lub Danych osobowych, każda osoba zobowiązana jest do:
      a) potwierdzenia tożsamości i uprawnień do uzyskania informacji przez rozmówcę
      b) niepozostawiania wiadomości zawierających Dane osobowe na automatycznych sekretarkach i poczcie głosowej,
      c) zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, w szczególności przed podaniem informacji lub jakichkolwiek danych upewnienie się czy rozmówca nie korzysta w obecności osób trzecich z zestawu lub trybu głośnomówiącego lub czy przebywa w otoczeniu umożliwiającym zachowanie poufności rozmowy,
      d) ograniczenia przesyłania dokumentów zawierających Dane osobowe lub informacje podlegające ochronie za pomocą faksów lub innych urządzeń niegwarantujących zachowania poufności korespondencji lub stwarzających duże ryzyko błędu przy wyborze odbiorcy;
   2) w trakcie kontaktów osobistych z osobami uprawnionymi do uzyskania informacji chronionych i przetwarzanych przez GDOŚ Danych osobowych, Pracownicy zobowiązani są do:
      a) zapewnienia właściwych warunków do przekazywania informacji, gwarantujących zachowanie poufności prowadzonej rozmowy oraz gwarantującej swobodę wypowiedzi – zaleca się korzystanie z pomieszczeń przeznaczonych do zapoznawania stron z dokumentami, sal konferencyjnych lub pomieszczeń biurowych GDOŚ, o ile zostaną zachowane inne warunki bezpieczeństwa,
      b) nieprzekazywania informacji i Danych osobowych w rozmowach prowadzonych w ciągach komunikacyjnych, windach, środkach komunikacji oraz innych miejscach publicznych, jeśli z treścią przekazywanych informacji mogłyby się zapoznać przypadkowe osoby postronne.

## § 7. Elektroniczna wymiana informacji

1. Informacje o najwyższych wymaganiach ochrony (tj. należące do IV klasy aktywów informacyjnych, np. wrażliwe dane osobowe) powinny być zaszyfrowane (np. przy użyciu archiwum 7zip z hasłem). Hasło musi być przekazywane osobną ścieżką transmisji, np. telefonicznie lub SMS-em, nigdy w tej samej wiadomości e-mail lub w kolejnej wiadomości.
2. Akta osobowe Pracowników przesyłane do odbiorców spoza GDOŚ powinny być zaszyfrowane (np. archiwum 7zip z hasłem). Hasło musi być przekazywane osobną ścieżką transmisji, np. telefonicznie lub SMS-em, nigdy w tej samej wiadomości e-mail lub w kolejnej wiadomości.
3. Nie należy otwierać podejrzanych załączników dołączonych do wiadomości e-mail (np. pliki wykonywalne o rozszerzeniu .exe, archiwa .zip). W sytuacji otrzymania wiadomości email z podejrzanym załącznikiem należy natychmiast zgłosić ten fakt do Pracownika Wydziału Informatyki BDG zgodnie z przyjętym w GDOŚ trybem zgłaszania.
4. Po odebraniu wiadomości e-mail należy każdorazowo upewnić się, że adres nadawcy jest prawidłowy. Nie należy otwierać załączników z wiadomości e-mail, pochodzącej od nieznanego nadawcy.
5. Podczas wysyłania wiadomości e-mail należy każdorazowo upewnić się, iż wpisany adres odbiorcy jest prawidłowy.
6. W przypadku wysyłania wiadomości e-mail do większej liczby osób poza GDOŚ, jeżeli jest to konieczne, należy zapewnić, aby osoby, do których skierowana jest tego typu korespondencja, nie miały możliwości zapoznania się z danymi pozostałych adresatów wiadomości – nie tylko ich imionami i nazwiskami, lecz także adresami e-mail. W tym celu adresy email adresatów umieszczać należy w polu „UDW”.
7. Zaleca się, aby maksymalny rozmiar załącznika wynosił 25MB, co zapewni, co do zasady, możliwość przesłania wiadomości e-mail i zaakceptowania jej przez serwer adresata.
8. Automatyczne przekazywanie wiadomości e-mail lub innych treści na zewnętrzny adres e-mail (spoza domeny gdos.gov.pl) bez zezwolenia pracownika Wydziału Informatyki BDG oraz Przełożonego jest zabronione.
9. Wymiana i przekazywanie informacji za pomocą szyfrowanego Nośnika danych (np. dysku twardego lub pendrive), może być realizowana wyłącznie za uprzednią zgodą pracownika Wydziału Informatyki BDG i Przełożonego.
10. Wykorzystanie rozwiązań podmiotu zewnętrznego służących do wymiany informacji może nastąpić tylko na podstawie zawartej z nim umowy, zgodnie z jej zapisami w tym zakresie.
11. W zakresie elektronicznej wymiany informacji obejmujących Dane osobowe obowiązują również zasady opisane w ***Polityce Przetwarzania Danych Osobowych.***

## § 8. Bezpieczne użytkowanie sprzętu i oprogramowania

1. Niedozwolone jest korzystanie z urządzeń służbowych i zasobów sieciowych do celów prywatnych.
2. Niedozwolone jest podłączanie urządzeń prywatnych do urządzeń lub sieci wewnętrznej GDOŚ.
3. Każdy Nośnik danych wydany uprawnionym użytkownikom Systemu teleinformatycznego GDOŚ, przed jego wydaniem do użytkowania, jest rejestrowany w ***Rejestrze Nośników informacji*** przez pracowników Wydziału Informatyki BDG. ***Rejestr Nośników informacji*** może być prowadzony w postaci elektronicznej lub przy wykorzystaniu oprogramowania do zarządzania zasobami informatycznymi w GDOŚ.

4. Podłączenie mobilnych urządzeń służbowych (np. notebooków) do sieci zewnętrznej (np. prywatna sieć domowa, sieć hotelowa, siec klienta) jest dozwolone tylko w celu nawiązania połączenia z siecią wewnętrzną GDOŚ za pośrednictwem VPN. Wszystkie odstępstwa od tego sposobu postępowania w uzasadnionych, wyjątkowych przypadkach, zatwierdza ABT.
5. Urządzenia mobilne i Nośniki danych, a tym samym informacje na nich przechowywane, muszą być odpowiednio chronione poprzez obowiązkowe szyfrowanie oraz utrzymywanie aktualnej kopii zapasowej danych na nich się znajdujących.
6. Przenośne Nośniki danych mogą być wykorzystywane wyłącznie do celów służbowych. Prywatne przenośne Nośniki danych nie mogą być podłączane do urządzeń czy infrastruktury GDOŚ. Wymiana danych za pośrednictwem przenośnych Nośników danych powinna zostać ograniczona do minimum. Szyfrowane, rejestrowane służbowe pamięci USB i dyski twarde są udostępniane wyłącznie przez pracowników Wydziału Informatyki BDG, które po użyciu należy zwrócić. Nośnik danych musi zostać bezpiecznie usunięty lub sformatowany przed ponownym wydaniem, za co odpowiadają pracownicy Wydziału Informatyki BDG.
7. Dozwolone jest zabieranie ze sobą stacji roboczych mobilnych (laptop, smartfon) w celach służbowych i wynoszenie ich poza siedzibę GDOŚ.
8. Zabronione jest samodzielne instalowanie oprogramowania na urządzeniach służbowych. Pracownicy Wydziału Informatyki BDG odpowiadają za dystrybucje dozwolonego oprogramowania i wsparcie w zakresie jego instalacji.
9. Do szyfrowania należy używać tylko oprogramowania zatwierdzonego i dostarczonego przez pracowników Wydziału Informatyki BDG.
10. Korzystając z urządzeń mobilnych poza siedzibą GDOŚ należy zadbać o to, aby dane wyświetlane na ekranie urządzenia nie były widoczne dla osób trzecich (np. w samolocie lub pociągu). Przekazywanie urządzeń służbowych osobom trzecim jest zabronione (nawet tymczasowo). Dozwolone jest używanie telefonów komórkowych i smartfonów w pojazdach silnikowych wyposażonych w zestaw głośnomówiący Bluetooth.
11. Użytkownik Systemu teleinformatycznego GDOŚ zobowiązany jest do gromadzenia danych i dokumentów zawierających Dane osobowe lub inne dane chronione w dedykowanej dla niego przestrzeni dyskowej serwera GDOŚ;
12. W pamięci wewnętrznej stacji roboczej lub mobilnego urządzenia komputerowego (laptop, tablet) użytkownik może gromadzić jedynie dokumenty i informacje niezbędne do bieżącej pracy, w tym niewypełnione druki formularzy, wzory dokumentów oraz dokumenty nie zawierające Danych osobowych, których ewentualna utrata lub kradzież nie będzie skutkować konsekwencjami prawnymi.
13. Obowiązuje całkowity zakaz gromadzenia w zasobach informatycznych GDOŚ danych niezwiązanych z wykonywaniem zadań na zajmowanym stanowisku służbowym, danych o charakterze prywatnym, zdjęć, filmów, plików muzycznych itp.
14. Nośniki danych oraz sprzęt informatyczny wydany użytkownikowi, a pozostający w zasobach GDOŚ, może podlegać kontroli, w tym kontroli zgromadzonych na nim danych i informacji. Do przeprowadzenia kontroli są upoważnieni pracownicy Wydziału Informatyki BDG, a także IOD w ramach realizacji zadań wynikających z art. 39 ust. 1 lit. b RODO.
15. Za bezpieczeństwo informacji, w tym Danych osobowych przetwarzanych z wykorzystaniem zasobów i Systemów teleinformatycznych GDOŚ, odpowiada każdy użytkownik Systemu informatycznego GDOŚ we właściwym dla siebie zakresie.

## § 9. Korzystanie z sieci publicznej Internet

1. Zabronione jest odwiedzanie stron internetowych, które zawierają treści potencjalnie szkodliwe lub niebezpieczne dla GDOŚ (np. pornografia, torrenty itp.).
2. W przypadku podejrzenia, że dostęp do sieci Internet nie był wykorzystywany zgodnie z przyjętymi w GDOŚ zasadami pracy, informacja ta przekazana zostanie do Przełożonego.
3. Zabronione jest zmienianie ustawień bezpieczeństwa przeglądarki internetowej skonfigurowanych przez pracowników Wydziału Informatyki BDG.
4. Zabrania się instalowania aplikacji lub aktualizacji oprogramowania. Takie czynności wykonują w GDOŚ wyłącznie pracownicy Wydziału Informatyki BDG.

## § 10. Dostęp zdalny

Zasady zarządzania dostępem zdalnym do informacji i zasobów GDOŚ opisane zostały w ***Regulaminie Pracy Zdalnej*.**

## § 11. Hasła

1. Wymagania dotyczące haseł użytkowników Systemu teleinformatycznego GDOŚ:
   1) hasło składa się z minimum 8 znaków;
   2) hasło powinno składać się z czterech typów znaków, którymi są małe i wielkie litery, cyfry i znaki specjalne (np. !@#);
   3) hasło nie może się powtarzać (kolejne hasła muszą być od siebie różne);
   4) hasła należy przechowywać w sposób gwarantujący ich poufność;
   5) w przypadku, gdy system nie umożliwia stosowania 2FA (dwuskładnikowego Uwierzytelnienia), hasło musi być zmieniane minimum co 90 dni.
2. Zabrania się tworzenia haseł na podstawie:
   1) cech i numerów osobistych (np. dat urodzenia, imion itp.);
   2) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx);
   3) identyfikatora, loginu użytkownika.
3. W przypadku pierwszego logowania do Systemu informatycznego GDOŚ, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, znane tylko jemu.
4. Jeśli dany system/aplikacja nie ma możliwości automatycznej, cyklicznej zmiany hasła, użytkownik zobowiązany jest do jego zmiany zgodnie z zasadami określonymi w ust. 1 i 2.
5. Zabrania się udostępniania haseł innym osobom. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą być natychmiast zmienione przez użytkownika lub właściwego ABT i AMS.
6. Zmiany hasła dokonuje użytkownik. W przypadku, gdy użytkownik zapomniał hasła, właściwy ABT i AMS ustawia hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania.
7. Zabrania się anonimowego logowania do Systemu teleinformatycznego GDOŚ.

8. Zabrania się przekazywania i przesyłania danych uwierzytelniających (login i/lub hasło) za pomocą telefonu, faksu ani poczty e-mail w formie jawnej.

## § 12. Bezpieczeństwo fizyczne

Zasady postępowania w zakresie zapewnienia bezpieczeństwa fizycznego opisane zostały w ***Zasadach bezpieczeństwa fizycznego*** obowiązujących w GDOŚ.

## § 13. Incydenty naruszenia bezpieczeństwa informacji

Zasady postępowania w przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji opisane zostały w ***Procedurze Zarządzania Incydentami***.

**Załącznik nr 4** do Zarządzenia nr 14 Generalnego Dyrektora Ochrony Środowiska w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska z dnia 17 listopada 2022 r.

# *Procedura nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Generalny Dyrektor Ochrony Środowiska

ANDRZEJ SZWEDA-LEWANDOWSKI

Generalny Dyrektor Ochrony Środowiska

.....

Generalny Dyrektor Ochrony Środowiska

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

1. Celem niniejszej procedury jest ustanowienie nadzoru nad dokumentacją niezbędną do wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI", oraz wsparcia skutecznego i efektywnego działania procesów w Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ".
2. Niniejsza procedura określa zasady nadzorowania dokumentacji SZBI w GDOŚ, a także opisuje sposób tworzenia, opiniowania, zatwierdzania, przeglądu i dystrybucji regulacji wewnętrznych w obszarze SZBI.

## § 2. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ;

2) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

3) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 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), którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

4) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;

5) **Komórce organizacyjnej** – należy przez to rozumieć biura i departamenty lub samodzielne stanowiska GDOŚ, określone w strukturze organizacyjnej GDOŚ;

6) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;

7) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.).

8) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ.

## § 3. Odpowiedzialność i uprawnienia

1. Pełnomocnik ds. BI odpowiada za:
   1) przegląd Dokumentacji SZBI, który dokonywany jest nie rzadziej niż co 12 miesięcy;
   2) w przypadku stwierdzenia konieczności dokonania zmian w Dokumentacji SZBI, określenie zakresu tych zmian;
   3) opracowanie propozycji zmian w Dokumentacji SZBI, polegające na sformułowaniu projektowanych postanowień Dokumentacji SZBI, z uwzględnieniem zakresu zmian wskazanego przez osoby, o których mowa w ust. 2 i 3;
   4) konsultacje, akceptacje lub odrzucenie propozycji zmian, o których mowa w pkt 3, opracowanych z właściwymi osobami lub komórkami organizacyjnymi w GDOŚ;
   5) przekazanie nowej wersji Dokumentacji SZBI do zatwierdzenia Dyrektora Generalnego GDOŚ;
   6) publikację nowej wersji Dokumentacji SZBI;
   7) rejestrowanie zmian w ***Rejestrze zmian w dokumentacji*** oraz odnotowywanie zmian w ***Karcie zmian dokumentu***;
   8) wdrażanie nowych wersji Dokumentacji SZBI;
   9) archiwizację, usunięcie lub zniszczenie wycofanych dokumentów SZBI;
   10) weryfikację wprowadzonych zmian w Dokumentacji SZBI;
   11) informowanie o lokalizacji Dokumentacji SZBI.
2. ABT odpowiada za bieżące monitorowanie SZBI w zakresie związanym z funkcjonowaniem bezpieczeństwa teleinformatycznego GDOŚ oraz, w razie zaistniałej potrzeby, określenie zakresu zmian w Dokumentacji SZBI, a także przedstawienie propozycji tych zmian Pełnomocnikowi BI.
3. KKO odpowiadają za bieżące monitorowanie SZBI w zakresie dotyczącym funkcjonowania danej komórki organizacyjnej oraz, w razie zaistniałej potrzeby, określenie zakresu zmian w Dokumentacji SZBI, a także przedstawienie ich Pełnomocnikowi BI.
4. IOD odpowiada za:
   1) bieżące monitorowanie SZBI w zakresie mającym wpływ na ochronę Danych osobowych oraz, w razie zaistniałej potrzeby, określenie zakresu zmian w Dokumentacji SZBI;
   2) przekazanie propozycji zmian do akceptacji Pełnomocnika BI zgodnie z ust. 1 pkt. 3-5.
5. Dyrektor Generalny GDOŚ odpowiada za zatwierdzenie bądź odmowę zatwierdzenia proponowanych zmian w dokumentacji SZBI.

## § 4. Forma dokumentacji SZBI

Dokumentacja SZBI GDOŚ ma postać papierową lub elektroniczną. W przypadku postaci elektronicznej dokumentacja jest przechowywana w systemie informatycznym GDOŚ, w sposób zapewniający jej identyfikowalność, bezpieczeństwo i dostępność dla uprawnionych osób.

## § 5. Nadzór nad dokumentacją

1. Każda zmiana w Dokumentacji SZBI powoduje konieczność wydania nowej wersji właściwych dokumentów, które były zmieniane. Zmiany w dokumentach dokonuje się na zasadach określonych w § 6 niniejszej procedury.
2. Po zatwierdzeniu nowej wersji Dokumentacji SZBI przez Dyrektora Generalnego GDOŚ, Pełnomocnik BI ma obowiązek opublikować ją w sieci *Intranet*, a następnie poinformować Pracowników o dokonanej zmianie oraz uzyskać od właściwych Pracowników potwierdzenie zapoznania się ze zmianami wprowadzonymi w Dokumentacji SZBI.
3. Nowe wersje dokumentów są rejestrowane w ***Rejestrze zmian w dokumentacji***, którego wzór stanowi załącznik nr 1 do niniejszej procedury, a ponadto są odnotowywane w ***Karcie zmian dokumentu*** umieszczonej na pierwszych stronach dokumentu.
4. Po przeprowadzeniu procedury, o której mowa w ust. 1-3, Pełnomocnik BI przystępuje do działań mających na celu wdrożenie zmian wprowadzonych w Dokumentacji SZBI.
5. Wycofany, nieaktualny egzemplarz dokumentu, oznaczony jako „dokument wycofany", przechowywany jest w systemie informatycznym GDOŚ w sposób zapewniający jego identyfikowalność i bezpieczeństwo, w miejscu zajmowanym przez Pełnomocnika BI.
6. Dokument wycofany jest rejestrowany w ***Rejestrze dokumentów wycofanych***, którego wzór stanowi załącznik nr 1 do niniejszej procedury.
7. Wycofane wersje dokumentów podlegają archiwizacji, usunięciu lub zniszczeniu na zasadach i po upływie okresu wynikających z odrębnych przepisów.

## § 6. Zasady zmian dokumentacji SZBI

1. Projekt dokumentu SZBI powinien być tworzony na bazie ***Szablonu dokumentu***, którego wzór stanowi załącznik nr 2 do niniejszej procedury.
2. Prace związane ze zmianami Dokumentacji SZBI prowadzi się w postaci elektronicznej, z uwzględnieniem następujących zasad:
   1) zmiany oraz uwagi wprowadza się w edytowalnej wersji projektów dokumentów podlegających modyfikacjom;
   2) zmiany w projektach dokumentów należy wprowadzać w trybie śledzenia zmian;
   3) uwagi w projektach dokumentów należy wprowadzać w formie komentarzy.
3. W toku prac związanych ze zmianami dokumentacji SZBI, Pełnomocnik BI może zwrócić się do poszczególnych komórek organizacyjnych lub osób, z prośbą o konsultację treści poszczególnych dokumentów, pozostających w ich właściwości.
4. Wszystkie modyfikacje prowadzone podczas konsultacji powinny być wykonywane w sposób pozwalający na identyfikację autora, daty oraz zagadnienia będącego przedmiotem modyfikacji, zaś projekty dokumentów powinny być przechowywane w sposób zapewniający ich identyfikowalność, bezpieczeństwo i dostępność dla uprawnionych osób.

## § 7. Sposób oznaczania oraz numerowania dokumentów

1. Każdy dokument SZBI jest identyfikowany nadaną mu nazwą, niepowtarzalnym numerem wersji oraz datą jego wydania.

2. Nazwa dokumentu powinna składać się co najmniej z określenia jego przedmiotu.
3. Każda nowa wersja Dokumentacji SZBI jest oznaczana kolejnym nowym numerem.

## § 8. Załączniki

Załącznikami do niniejszej procedury są:

1) załącznik nr 1 – Rejestr zmian w dokumentacji/ Rejestr dokumentów wycofanych;
2) załącznik nr 2 – Szablon dokumentu Systemu Zarządzania Bezpieczeństwem Informacji;
3) załącznik nr 3 – Plan dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

*Załącznik nr 1 do Procedury nadzoru nad dokumentacją*

# *Rejestr zmian w dokumentacji /Rejestr dokumentów wycofanych*

| Obszar zmian | Komórka nadzorująca obszar | Zakres i powód zmiany/wycofania | Dokumenty / wytyczne podlegające zmianie/wycofaniu | Identyfikator nowej wersji | Data wejścia w życie nowej wersji |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

*Załącznik nr 2 do Procedury nadzoru nad dokumentacją*

# *Szablon dokumentu Systemu Zarządzania Bezpieczeństwem Informacji*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

……..

# [*Nazwa dokumentu*]

ZATWIERDZAM

……..

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

## Spis treści

## § 1. Cel

Celem dokumentu jest:

1. […]
2. […]

## § 2. Zakres

Niniejszy dokument stosują:

3. […]

Dokument ma zastosowanie do informacji chronionych:

4. Formy [papierowej] [elektronicznej].

## § 3. Terminologia

Pojęcia używane w niniejszej procedurze oznaczają:

Termin – [opis]

## § 4. Odpowiedzialność i uprawnienia

1. […]

## § 5. Zasady i opis postępowania

1. […]

## § 6. Zasady i opis postępowania

1. […]

## § 7. Lista dokumentów związanych

1. […]

## § 8. Załączniki

1. […]

*Załącznik nr 3 do Procedury nadzoru nad dokumentacją*

# *Plan dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji Generalnej Dyrekcji Ochrony Środowiska*

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem niniejszego dokumentu jest wskazanie zalecanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI", tworzącej zasady bezpieczeństwa i zapewniającej skuteczność na poziomie znajomości i stosowania zasad przez wszystkie grupy odbiorców z uwzględnieniem obowiązującego stanu prawnego w szczególności do postanowień:

1) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070, z późn. zm.);
2) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), zwanego dalej „rozporządzeniem KRI";
3) 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 z 04.05.2016, str. 1), zwanego dalej „RODO";
4) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
5) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z późn. zm.);
6) normy ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 oraz ISO/IEC 22301.

## § 2. Zakres

1. W skład dokumentacji SZBI wchodzą: Główne dokumenty SZBI, Procedury Bezpieczeństwa, a także pozostałe dokumenty SZBI.
2. Niniejszy dokument stosują osoby odpowiedzialne za opracowywanie i aktualizację dokumentacji SZBI w Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ".

# Plan dokumentacji

| L.P. | Nazwa dokumentu | Opis dokumentu | Podstawa prawna lub nr normy | Pełny dostęp do dokumentu | Dostęp do odczytu |
|---|---|---|---|---|---|
| **Główne dokumenty SZBI** | | | | | |
| 1. | Polityka Bezpieczeństwa Informacji (PBI) | Dokument określający strategię, podstawy przetwarzania i zobowiązania do przestrzegania zasad bezpieczeństwa.<br>Celem Polityki Bezpieczeństwa Informacji jest ustanowienie SZBI w GDOŚ. | ISO/IEC 27001 A.5<br>ISO/IEC 27001 5 | Pełnomocnik ds. BI | Wszystkie zainteresowane strony |
| 2. | Polityka Bezpieczeństwa Teleinformatycznego (PBT) | Dokument określający zasady utrzymywania poufności, integralności oraz dostępności systemów teleinformatycznych. Wskazuje zasady utrzymania ciągłości aplikacji i usług informatycznych i zobowiązania do utrzymania parametrów systemów adekwatnych do działalności GDOŚ.<br>Polityka Bezpieczeństwa Teleinformatycznego jest dokumentem opracowanym w celu przedstawienia sposobu zarządzania bezpieczeństwem kluczowych elementów systemów informatycznych. | ISO 22301 5<br>ISO/IEC 27001 A.5<br>ISO/IEC 27001 A.8-A.18<br>ISO/IEC 22301 8<br>RODO art. 24, art. 25, art. 32 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Administrator Merytoryczny Systemu<br>Inspektor Ochrony Danych | Pracownicy Zespołu ds. Informatyki w Biurze Dyrektora Generalnego GDOŚ<br>Wszystkie osoby upoważnione przez Dyrektora Generalnego GDOŚ |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 3. | Polityka Przetwarzania Danych Osobowych (PPDO) | Dokument wskazujący wymagania dla ochrony danych osobowych.<br>Polityka ta opisuje ogólne zasady ochrony danych osobowych obowiązujące w GDOŚ oraz role i zadania osób uczestniczących w procesie przetwarzania informacji oraz ochrony danych osobowych. | ISO/IEC 27001 A.18<br>RODO art. 24 | Pełnomocnik ds. BI<br>Inspektor Ochrony Danych | Wszystkie osoby upoważnione przez Dyrektora Generalnego GDOŚ |
| **Procedury Bezpieczeństwa** | | | | | |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 4. | Procedura nadzoru nad dokumentacją | Procedura uzupełniona o zasady postępowania oraz nadzoru nad dokumentacją i zapisami SZBI. Procedura ma na celu zapewnienie ujednoliconego sposobu opracowywania dokumentacji SZBI pod względem formy i układu treści, aby zapewnić jej formalną i merytoryczną spójność.<br>Celem procedury jest ustanowienie nadzoru nad dokumentacją niezbędną do wdrożenia i utrzymania SZBI oraz dla wsparcia skutecznego i efektywnego działania procesów w GDOŚ. Procedura określa zasady i tryb nadzorowania dokumentów SZBI, a także opisuje sposób tworzenia, opiniowania, zatwierdzania, przeglądu i dystrybucji przepisów wewnętrznych w obszarze SZBI. | ISO/IEC 27001 7 | Pełnomocnik ds. BI | Wszyscy pracownicy i współpracownicy GDOŚ<br>Podmioty i instytucje upoważnione na podstawie przepisów prawa |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 5. | Procedura zarządzania ryzykiem wraz z metodyką szacowania ryzyka | Procedura ma na celu ustalenie odpowiedzialności w zakresie zarządzania ryzykiem w bezpieczeństwie informacji, określenie zasad inwentaryzowania aktywów oraz zasad szacowania ryzyka bezpieczeństwa informacji i ochrony danych osobowych.<br>Celem procedury jest ustalenie odpowiedzialności w zakresie zarządzania ryzykiem dla ochrony informacji w GDOŚ, określenie zasad klasyfikacji oraz zasad szacowania ryzyka dla ochrony informacji i ochrony danych osobowych w GDOŚ. | ISO/IEC 27001 6 i 8<br>ISO/IEC 27001 A.8<br>ISO/IEC 27005<br>ISO/IEC 22301 6 i 8<br>RODO Art. 32 | Pełnomocnik ds. BI<br>Inspektor Ochrony Danych | Wszyscy pracownicy i współpracownicy GDOŚ |
| 6. | Procedura kontroli dostępu do aktywów informacyjnych | Celem procedury jest ustalenie zasad kontroli dostępu oraz ochrona przed naruszeniami bezpieczeństwa. | ISO/IEC 27001 A.9<br>ISO/IEC 27001 A.7 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Administrator Merytoryczny Systemu | Inspektor Ochrony Danych<br>Kierownicy Komórek Organizacyjnych<br>Pracownicy Zespołu ds. Informatyki w Biurze Dyrektora Generalnego GDOŚ |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 7. | Procedura zarządzania incydentami bezpieczeństwa informacji, w tym danych osobowych | Procedura określa postępowanie w sytuacji naruszenia bezpieczeństwa oraz wypełnienia obowiązku w zakresie zgłaszania incydentów:<br>1) cyberbezpieczeństwa do CSIRT;<br>2) naruszeń ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych.<br>Celem procedury jest określenie postępowania w sytuacji naruszenia ochrony informacji w GDOŚ, a także wypełnienie obowiązku w zakresie zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu, o którym mowa w art. 33 RODO | ISO/IEC 27001 A.16<br>ISO/IEC 27035<br>RODO art. 33 | Pełnomocnik ds. BI<br>Inspektor Ochrony Danych | Wszyscy pracownicy i współpracownicy GDOŚ |
| 8. | Procedura pomiaru i oceny skuteczności zabezpieczeń | Procedura reguluje zakres monitorowania bezpieczeństwa informacji. Określa wskaźniki i częstotliwość raportowania wyników do Pełnomocnika ds. BI.<br>Celem niniejszej procedury jest ustalenie zasad monitorowania i pomiaru zabezpieczeń. | ISO/IEC 27001 9<br>RODO art. 32, art. 39 | Pełnomocnik ds. BI<br>Inspektor Ochrony Danych | Kierownicy Komórek Organizacyjnych<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Podmioty i instytucje upoważnione na podstawie przepisów prawa |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 9. | Procedura zarządzania poprawkami | Procedura określa sposób i mechanizmy identyfikacji podatności systemów teleinformatycznych. Jednocześnie wskazuje zasady aktualizacji i instalacji poprawek bezpieczeństwa dla systemów i aplikacji, wskazuje odpowiedzialność za aktualizacje, a także zasady oceny wpływu poprawek i aktualizacji na ciągłość działania systemów. | ISO/IEC 27001 A.12 | Pełnomocnik ds. BI | Administrator Bezpieczeństwa Teleinformatycznego<br>Pracownicy Zespołu ds. informatyki w Biurze Dyrektora Generalnego GDOŚ<br>Pracownicy podmiotów zewnętrznych odpowiedzialnych za obsługę IT |
| 10. | Procedura zarządzania ciągłością działania systemu teleinformatycznego | Procedura definiuje proces utrzymania ciągłości, zasady redundancji i identyfikację pojedynczych punktów awarii oraz tworzenie i testowanie planów ciągłości oraz instrukcji Disaster Recovery.<br>Celem procedury jest ustalenie zasad postępowania w procesie zarządzania ciągłością działania i przeciwdziałanie przerwom w funkcjonowaniu systemu oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie. | ISO/IEC 27001 A.17<br>ISO 22301 5 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego | Kierownicy Komórek Organizacyjnych<br>Pracownicy Zespołu ds. informatyki w Biurze Dyrektora Generalnego GDOŚ<br>Właściciele procesów<br>Wszystkie osoby upoważnione przez Dyrektora Generalnego GDOŚ, w tym pracownicy podmiotów odpowiedzialnych za utrzymanie systemu informatycznego |

# Plan dokumentacji

| L.P. | Nazwa dokumentu | Opis dokumentu | Podstawa prawna lub nr normy | Pełny dostęp do dokumentu | Dostęp do odczytu |
|---|---|---|---|---|---|
| 11. | Procedura wykonywania kopii zapasowych | Procedura tworzenia kopii zapasowych określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji. Celem dokumentu jest:<br>1) Ustalenie zasad postępowania w procesie wykonywania kopii zapasowych;<br>2) Ochrona przed utratą danych w celu zapewnienia wznowienia działalności w wypadku awarii infrastruktury informatycznej.<br>Celem procedury jest ustalenie zasad postępowania w procesie wykonywania kopii zapasowych w systemie teleinformatycznym oraz ochrona krytycznych procesów przed utratą danych w celu zapewnienia wznowienia działalności w wypadku awarii infrastruktury przechowującej dane. | ISO/IEC 27001 A.12<br>RODO art. 32 | Pełnomocnik ds. BI | Administrator Bezpieczeństwa Teleinformatycznego<br>Pracownicy Zespołu ds. Informatyki w Biurze Dyrektora Generalnego GDOŚ |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 12. | Procedura niszczenia nośników oraz przekazywania do ponownego użycia | Celem dokumentu jest opisanie sposobu postępowania w sytuacji konieczności przekazania aktywów do ponownego użycia oraz w sytuacji konieczności zniszczenia nośnika informacji. | ISO/IEC 27001 A.8<br>ISO/IEC 21964 | Pełnomocnik ds. BI<br>Inspektor Ochrony Danych | Administrator Bezpieczeństwa Teleinformatycznego<br>Pracownicy Zespołu ds. informatyki w Biurze Dyrektora Generalnego GDOŚ<br>Właściciele aktywów<br>Kierownicy Komórek Organizacyjnych<br>Podmioty i instytucje upoważnione na podstawie przepisów prawa |
| 13. | Procedura zarządzania konfiguracją i zmianami systemu teleinformatycznego | Celem dokumentu jest zdefiniowanie zasad zarządzania zmianami wprowadzanych w konfiguracji urządzeń i oprogramowania. Procedurę należy stosować do wszystkich systemów informatycznych obecnych i w przyszłości wdrażanych i rozwijanych przez GDOŚ. | ISO/IEC 27001 A.12 | Pełnomocnik ds. BI | Administrator Bezpieczeństwa Teleinformatycznego<br>Administrator Merytoryczny Systemu<br>Pracownicy Zespołu ds. Informatyki w Biurze Dyrektora Generalnego GDOŚ |

# Plan dokumentacji

| L.P. | Nazwa dokumentu | Opis dokumentu | Podstawa prawna lub nr normy | Pełny dostęp do dokumentu | Dostęp do odczytu |
|---|---|---|---|---|---|
| **Pozostałe dokumenty SZBI** | | | | | |
| 14. | Zasady bezpieczeństwa fizycznego | Celem dokumentu jest określenie minimalnych wymagań bezpieczeństwa fizycznego i środowiskowego w pomieszczeniach z infrastrukturą centralną systemów informatycznych – pomieszczenie serwerowni oraz określenie zasad dostępu do pomieszczeń, jak również zasad zabezpieczeń pomieszczeń GDOŚ. | ISO/IEC 27001 A.11 | Pełnomocnik ds. BI | Administrator Bezpieczeństwa Teleinformatycznego<br>Pracownicy Zespołu ds. Informatyki w Biurze Dyrektora Generalnego GDOŚ |

# Plan dokumentacji

| L.P. | Nazwa dokumentu | Opis dokumentu | Podstawa prawna lub nr normy | Pełny dostęp do dokumentu | Dostęp do odczytu |
|---|---|---|---|---|---|
| 15. | Regulamin Bezpieczeństwa Informacji | Regulamin stanowi zestaw zasad postępowania dla osób mających dostęp do informacji chronionych GDOŚ, w szczególności:<br>1) Zasady bezpieczeństwa oraz unikania zagrożeń;<br>2) Stosowanie skutecznych sposobów zabezpieczania się przed zagrożeniami bezpieczeństwa podczas korzystania z systemów teleinformatycznych;<br>3) Zasady postępowania z incydentami.<br>4) Zasady unikania zagrożeń przy korzystania z usług internetowych;<br>5) Obowiązki i zasady postępowania wynikające z procedur bezpieczeństwa w zakresie niezbędnym do prawidłowego wykonywania obowiązków przez pracowników i współpracowników;<br>6) Język dokumentu powinien zapewniać osobom niebędącym specjalistami w dziedzinie bezpieczeństwa informacji zrozumienie i wyjaśnienie wprowadzonych regulacji dotyczących bezpieczeństwa systemów. | ISO/IEC 27001 A.7-A.13, A.16, A.18<br>RODO art. 7-22, art. 33, art. 39 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Inspektor Ochrony Danych | Wszystkie osoby uzyskujące dostęp do informacji chronionych GDOŚ |

# Plan dokumentacji

| L.P. | **Nazwa dokumentu** | **Opis dokumentu** | **Podstawa prawna lub nr normy** | **Pełny dostęp do dokumentu** | **Dostęp do odczytu** |
|---|---|---|---|---|---|
| 16. | Zasady bezpieczeństwa informacji w relacjach z dostawcami | Dokument ten stanowi zestaw minimalnych wymagań bezpieczeństwa dla podmiotów zewnętrznych mających dostęp do zasobów informacyjnych GDOŚ. | ISO/IEC 27001 A.15 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Inspektor Ochrony Danych | Wszystkie zainteresowane strony |
| 17. | Słownik pojęć używanych w dokumentach SZBI | Pojęcia używane w dokumentacji SZBI. | ISO/IEC 27000<br>RODO art. 4 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Inspektor Ochrony Danych | Wszystkie zainteresowane strony |
| 18. | Deklaracja stosowania | Deklaracja stosowania zabezpieczeń zgodnie z ISO/IEC 27001 to kluczowy dokument SZBI.<br>Deklaracja stosowania to obowiązkowy dokument, który należy sporządzić w systemie zarządzania bezpieczeństwem informacji ISO/IEC 27001. | ISO/IEC 27001 6 | Pełnomocnik ds. BI<br>Administrator Bezpieczeństwa Teleinformatycznego<br>Inspektor Ochrony Danych | Wszystkie zainteresowane strony |

**Załącznik nr 5** do Zarządzenia nr 14 Generalnego Dyrektora Ochrony Środowiska w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska z dnia 17 listopada 2022 r.

# *Procedura zarządzania Incydentami bezpieczeństwa informacji, w tym danych osobowych w Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Generalny Dyrektor Ochrony Środowiska

ANDRZEJ SZWEDA-LEWANDOWSKI

Generalny Dyrektor Ochrony Środowiska

.....

Generalny Dyrektor Ochrony Środowiska

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

1. Celem procedury jest:

   1) określenie postępowania w sytuacji naruszenia ochrony informacji w GDOŚ;

   2) wypełnienie obowiązku w zakresie zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu, o którym mowa w art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/79 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 z 04.05.2016, str. 1), zwanego dalej „RODO";

   3) wypełnienie obowiązku w zakresie zgłaszania Incydentów cyberbezpieczeństwa wynikającego z art. 22 ust 1 ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z późn. zm.).

2. GDOŚ w procesie zarządzania Incydentami kładzie nacisk na ustanowienie zdolności reagowania na Incydenty oraz zapobiegania Incydentom poprzez zapewnienie, że Systemy teleinformatyczne, sieci i aplikacje są wystarczająco bezpieczne.

## § 2. Zakres

Niniejszą procedurę należy stosować do wszystkich Incydentów związanych z bezpieczeństwem informacji.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.

2) **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem Danych Osobowych jest Generalny Dyrektor Ochrony Środowiska, w imieniu którego zadania realizuje Dyrektor Generalny GDOŚ. W zakresie przetwarzania danych osobowych osób zatrudnionych w GDOŚ Administratorem Danych Osobowych jest Generalna Dyrekcja Ochrony Środowiska w imieniu której funkcję ADO wykonuje Dyrektor Generalny GDOŚ.

3) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną.

4) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. NICK, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby

fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań

5) **Incydencie** – należy przez to rozumieć pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań GDOŚ i zagrażają bezpieczeństwu informacji.

6) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 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), którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

7) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.

8) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);

9) **Przełożonym** – należy przez to rozumieć bezpośredniego zwierzchnika;

10) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ;

## § 4. Odpowiedzialność i uprawnienia

1. Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**
2. Zespół do spraw Zarządzania Bezpieczeństwem Informacji, zwany dalej **„Zespołem ds. ZBI”**, odpowiada za wsparcie Pełnomocnika ds. BI w zakresie obsługi Incydentu.
3. Za współpracę z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV odpowiada osoba wyznaczona przez Dyrektora Generalnego GDOŚ, zwana dalej **„Punktem kontaktowym”**.

## § 5. Proces zarządzania Incydentami

1. Incydentami są w szczególności:
   1) nieupoważniony dostęp, modyfikacja, kopiowanie lub zniszczenie danych, w tym danych osobowych, w Systemie teleinformatycznym, na nośnikach papierowych i elektronicznych;
   2) zmiana lub brak zawartości zbioru danych, w tym danych osobowych uniemożliwiających w szczególności ustalenie tożsamości osoby, której dane dotyczą;
   3) udostępnianie danych, w tym danych osobowych, nieuprawnionym podmiotom lub osobom;

4) nielegalne lub nieświadome ujawnienie danych, w tym danych osobowych;
5) nieuprawnione pozyskiwanie danych, w tym danych z nielegalnych źródeł;
6) dostęp osób nieuprawnionych do pomieszczeń, w których przetwarza się dane, lub brak nadzoru nad osobami nieuprawnionymi przebywającymi w tych pomieszczeniach (np. serwisanci z firm zewnętrznych);
7) wykrycie niezabezpieczonego kanału udostępniania danych;
8) częściowy lub całkowity brak dostępu do systemu teleinformatycznego lub dostęp w zakresie szerszym niż wynikający z przyznanych uprawnień;
9) praca Systemu teleinformatycznego odbiegająca od normalnej;
10) podejrzenie lub stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność Systemu teleinformatycznego;
11) ujawnienie indywidualnych haseł dostępu do systemu;
12) przesłanie danych przez Internet bez zabezpieczenia;
13) korzystanie z nośników elektronicznych z danymi bez ich zabezpieczenia – szyfrowania;
14) wykonywanie nieuprawnionych kopii danych, w tym danych osobowych, lub naruszenie bezpieczeństwa tych kopii (niewłaściwe przechowywanie lub niszczenie nośników zewnętrznych);
15) podejrzenie kradzieży sprzętu komputerowego, oprogramowania, nośników zewnętrznych lub dokumentów zawierających dane, w tym dane osobowe;
16) naruszenie zasad ochrony fizycznej pomieszczeń (np. zauważenie śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf).

2. Etapy procesu zarządzania Incydentami to:
   1) Przygotowanie;
   2) Wykrywanie oraz zgłaszanie podejrzenia wystąpienia Incydentu;
   3) Analiza;
   4) Powstrzymywanie, eliminacja i odzyskiwanie;
   5) Działania po Incydencie.
3. W ramach etapu **Przygotowanie** realizuje się działania zgodnie z poniższymi wytycznymi:
   1) osoby obsługujące Incydenty w GDOŚ powinny być wyposażone w odpowiednie zasoby i narzędzia zapewniające zdolność do reagowania na Incydent. W związku z tym GDOŚ powinna posiadać:
      a) wiele środków komunikacji i koordynacji na wypadek awarii jednego mechanizmu, (np.: telefony komórkowe używane przez członków Zespołu ds. ZBI poza godzinami pracy oraz do komunikacji w miejscu pracy),
      b) system monitorowania spraw do śledzenia informacji o Incydentach, ich statusu itp.,
      c) bezpieczny magazyn do przechowywania dowodów i innych wrażliwych materiałów;
   2) GDOŚ powinna posiadać sprzęt i oprogramowanie do obsługi Incydentów:
      a) urządzenia do tworzenia kopii zapasowych w celu tworzenia obrazów dysków, zachowywania plików dziennika i zapisywania innych istotnych danych dotyczących Incydentów,

b) zapasowe stacje robocze, serwery i sprzęt sieciowy lub zwirtualizowane odpowiedniki, które mogą być używane do wielu celów, takich jak przywracanie kopii zapasowych i testowanie złośliwego oprogramowania,

c) czyste nośniki wymienne,

d) sniffer pakiety i analizatory protokołów do przechwytywania i analizowania ruchu sieciowego,

e) akcesoria do gromadzenia dowodów (np. notatniki w twardej oprawie, aparaty cyfrowe, nagrywarki audio, celem zachowania dowodów w razie podjęcia działań prawnych).

3) GDOŚ powinna posiadać zasoby do analizy Incydentów, w szczególności dokumentację systemów operacyjnych, aplikacji, protokołów oraz produktów do wykrywania włamań i programów antywirusowych, diagramy sieciowe, listę kluczowych zasobów takich jak serwery baz danych. W zakresie oprogramowania do łagodzenia skutków Incydentów GDOŚ powinna posiadać dostęp do obrazów czystego systemu operacyjnego i instalacji aplikacji w celu przywracania i odzyskiwania systemu;

4) w ramach obsługi Incydentu w GDOŚ Zespół ds. ZBI może korzystać z zestawów wcześniej przygotowanych zasobów do obsługi Incydentów, obejmujących elementy wskazane w pkt 3, w szczególności każdy zestaw może obejmować laptop z odpowiednim oprogramowaniem (np. snifferami pakietów, oprogramowaniem do informatyki śledczej), a także urządzenia do tworzenia kopii zapasowych, czyste nośniki oraz podstawowy sprzęt i kable sieciowe;

4. W ramach etapu **Wykrywanie oraz zgłaszanie podejrzenia wystąpienia Incydentu** działania podejmowane są zgodnie z poniższą procedurą:

1) wszyscy Pracownicy mają obowiązek natychmiastowego zgłaszania każdego podejrzenia wystąpienia Incydentu;

2) źródłem informującym o podejrzeniu wystąpienia Incydentu w GDOŚ może być także podmiot zewnętrzny mający dostęp do Aktywów informacyjnych GDOŚ oraz CSIRT GOV, jak również każda inna osoba, która posiada wiedzę o wystąpieniu takiego zdarzenia;

3) w przypadku podejrzenia wystąpienia Incydentu zgłoszenie może być dokonane osobiście do Pełnomocnika ds. BI, za pośrednictwem poczty elektronicznej na adres: incydent@gdos.gov.pl lub telefonicznie. Numer telefonu przeznaczony do zgłaszania Incydentów jest udostępniony w sieci Intranet. Odpowiedzialnym za jego udostępnienie oraz aktualizację jest pełnomocnik ds. BI

4) w przypadku gdy Incydent dotyczy danych osobowych zgłoszenie należy przekazać także do IOD, osobiście, za pośrednictwem poczty elektronicznej na adres: inspektor.ochrony.danych@gdos.gov.pl lub telefonicznie na numer wskazany w sieci Intranet. Numer telefonu przeznaczony do zgłaszania Incydentów jest udostępniony w sieci Intranet. Odpowiedzialnym za jego udostępnienie oraz aktualizację jest IOD.

5) Niezależnie od obowiązku wskazanego w pkt 3) i 4), Pracownik każdorazowo jest zobowiązany do poinformowania o podejrzeniu wystąpienia Incydentu swojego Przełożonego;

6) dokonując zgłoszenia podejrzenia wystąpienia Incydentu należy podać imię i nazwisko i służbowy adres e-mail osoby zgłaszającej, a ponadto informacje umożliwiające ustalenie okoliczności związanych z wystąpieniem Incydentu, w szczególności, jeżeli są znane:

a) opis zdarzenia (np. kiedy Incydent się rozpoczął, kiedy został wykryty, zgłoszony, zakończony);

b) fizyczną lokalizację Incydentu (np. miejscowość, adres lokalu, numer pomieszczenia);

c) aktualny stan Incydentu (np. trwający atak);

d) źródło lub przyczynę Incydentu, w tym nazwy hostów i adresy ip; (w jaki sposób Incydent został wykryty, co się stało);

e) opis zasobów, których dotyczył Incydent (np. sieci, hosty, aplikacje, dane), w tym nazwy hostów systemów, adresy IP i funkcje;

f) jeśli są znane, kategoria Incydentu, wektory ataku związane z Incydentem oraz wskaźniki związane z Incydentem (np. wzorce ruchu, klucze rejestru itp.);

g) czynniki priorytetyzacji (np. wpływ funkcjonalny, wpływ informacji, możliwość odzyskania itp.);

h) czynniki łagodzące (np. informacje o zabezpieczeniach posiadanych przez sprzęt);

i) wykonane działania w odpowiedzi na Incydent (np. wyłączenia hosta, odłączenie hosta od sieci);

j) organizacje, z którymi się skontaktowano (np. dostawca oprogramowania),

k) ewentualne wstępne zakwalifikowanie Incydentu,

l) ścieżkę dostępu, logi i inne dane lokalizujące Incydent,

m) spostrzeżenia zgłaszającego Incydent,

n) podjęte środki minimalizujące Incydent.

7) dokonując zgłoszenia Incydentu związanego z bezpieczeństwem danych osobowych należy podać imię i nazwisko i służbowy adres e-mail osoby zgłaszającej, a ponadto informacje umożliwiające ustalenie okoliczności związanych z wystąpieniem Incydentu, w szczególności, jeżeli są znane:

a) datę wystąpienia i ujawnienia Incydentu;

b) liczbę osób, których Incydent dotyczy;

c) kategorię osób, których dotyczy Incydent (np. Pracownicy, strony postępowania);

d) rodzaj danych, których dotyczy Incydent (np. imiona i nazwiska, numery PESEL, dane adresowe);

e) opis Incydentu;

f) informację czy Incydent ma związek z wykorzystywaniem do przetwarzania zasobów informatycznych GDOŚ;

g) osoby zawiadomione o Incydencie i czas zawiadomienia;

h) kontakt bezpośredni do osoby zawiadamiającej o Incydencie;

8) w przypadku wystąpienia Incydentu Pracownik jest zobowiązany:

a) postępować zgodnie z instrukcjami Pełnomocnika ds. BI, Przełożonego, IOD lub ABT,

b) niezwłocznie przystąpić do zapobieżenia dalszym zagrożeniom lub zmniejszeniu niepożądanych skutków zaistniałego Incydentu,

c) zabezpieczyć sprzęt komputerowy i dokumenty, a w szczególności nie wyłączać komputera bez zgody Pełnomocnika ds. BI,

d) zabezpieczyć ewentualne dowody zdarzenia, w szczególności wydruk lub zrzut ekranu monitora, kopie lub wydruki dokumentów,

e) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia,

f) w szczególnych przypadkach przerwać przetwarzanie Aktywów Informacyjnych (np.: zaprzestać pracy w Systemie teleinformatycznym);

9) w zależności od charakteru Incydentu (bezpieczeństwo fizyczne, bezpieczeństwo teleinformatyczne, bezpieczeństwo danych osobowych) odpowiedni członek Zespołu ds. ZBI zarządza działaniami mającymi na celu minimalizację skutków wystąpienia danego Incydentu;

10) Pełnomocnik ds. BI prowadzi ***Rejestr Incydentów związanych z bezpieczeństwem informacji***, którego wzór jest określony w załączniku nr 1 do niniejszej procedury;

11) ABT może prowadzić ***Rejestr Incydentów zaistniałych w systemach teleinformatycznych***, którego wzór jest określony w załączniku nr 1 do niniejszej procedury;

12) IOD prowadzi ***Rejestr naruszeń ochrony danych osobowych***, którego wzór jest określony w załączniku nr 2 do niniejszej procedury;

13) W przypadku naruszenia zasad bezpieczeństwa informacji i danych osobowych, skutkującego wysokim ryzykiem naruszenia praw i wolności osób fizycznych, ADO zawiadamia o zaistniałym zdarzeniu osoby, których dane dotyczą i informuje o związanym z tym zdarzeniem ryzykiem dla bezpieczeństwa naruszenia ich danych;

14) Zawiadomienie, o którym mowa w pkt 13, powinno zawierać elementy, o których mowa w art. 33 ust. 3 lit. b, c i d RODO. Zawiadomienia dokonuje się bez zbędnej zwłoki i można tego dokonać poprzez:

a) wysłanie indywidualnych zawiadomień do osób, których dane zostały zagrożone (drogą elektroniczną lub korespondencją pocztową, za potwierdzeniem odbioru);

b) ogłoszenia prasowe lub publikacja na stronach internetowych, jeśli koszty zawiadomień indywidualnych były niewspółmiernie wysokie do założonego celu.

Wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy rozumieć w szczególności jako ujawnienie, zniszczenie lub kradzież danych i informacji:

a) o których mowa w art 9 i 10 RODO - np. dane o stanie zdrowia, o przynależności do związków zawodowych, o wyrokach skazujących lub czynach zabronionych ;

b) umożliwiających kradzież tożsamości osoby fizycznej (np. dane identyfikacyjne, w tym numer ewidencyjny PESEL, numer dokumentu tożsamości itp.);

c) umożliwiających zaciągnięcie zobowiązań finansowych w imieniu osoby fizycznej (dane identyfikacyjne, w tym numer ewidencyjny PESEL, numer dokumentu tożsamości itp.);

15) Dyrektor Generalny GDOŚ zawierając umowę, w ramach której podmiot zewnętrzny uzyskuje dostęp do Aktywów Informacyjnych, zawiera w niej zasady postępowania w sytuacji wystąpienia Incydentu oraz zobowiązuje podmiot zewnętrzny do bezwzględnego ich stosowania. Minimalne wymagania bezpieczeństwa dla podmiotów zewnętrznych, które powinny zostać uwzględnione w umowach, zostały zawarte w dokumencie ***Zasady bezpieczeństwa informacji w relacjach z dostawcami.*** Każdy pracownik podmiotu zewnętrznego zgłasza Incydent do GDOŚ poprzez wybrany kanał zgłoszenia, określony w umowie z podmiotem zewnętrznym. Zgłoszenie powinno nastąpić nie później niż w ciągu 60 minut po stwierdzeniu faktu wystąpienia Incydentu oraz zawierać:

a) odwołanie do numeru zawartej umowy;

b) opis okoliczności zdarzenia, a w przypadku naruszenia ochrony danych osobowych opisywać także 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;

c) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

d) możliwe konsekwencje naruszenia ochrony danych osobowych;

e) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków mających na celu zminimalizowanie jego ewentualnych negatywnych skutków.

16) W przypadku wykrycia Incydentu przez CSIRT GOV oraz poinformowaniu o tym Punktu kontaktowego, Punkt Kontaktowy powiadamia o tym fakcie Pełnomocnika ds. BI oraz pozostałych członków Zespołu ds. ZBI, jak również Dyrektora Generalnego GDOŚ.

5. W ramach etapu **Analiza** działania podejmowane są zgodnie z poniższymi wytycznymi:

1) przyczyny wystąpienia Incydentu muszą być analizowane, a mechanizmy bezpieczeństwa odpowiednio modyfikowane w celu zminimalizowania ryzyka ponownego wystąpienia przypadków naruszenia bezpieczeństwa informacji;

2) Zespół ds. ZBI poddaje analizie każdy przypadek zaistniałego Incydentu i, o ile zajdzie taka konieczność, określa działania naprawcze;

3) w przypadku stwierdzenia Incydentu Zespół ds. ZBI niezwłocznie przeprowadza wstępną analizę Incydentu, w celu określenia jego zakresu. W tym celu, w szczególności Zespół ds. ZBI ustala których sieci, systemów lub aplikacji dotyczy Incydent, kto lub co spowodowało Incydent, a także w jaki sposób doszło do jego wystąpienia. (np. jakie narzędzia lub metody ataku zostały użyte, jakie luki w zabezpieczeniach zostały wykorzystane).

4) Wstępna analiza, o której mowa w pkt 3), powinna dostarczyć Zespołowi ds. ZBI informacji wystarczających do ustalenia priorytetów dalszych działań, takich jak powstrzymanie Incydentu i głębsza analiza skutków Incydentu.

5) mając na uwadze skuteczność analizy Incydentów należy wykorzystać wytyczne i standardy określone zawarte w *Narodowym Standardzie Cyberbezpieczeństwa - Podręczniku postępowania z Incydentami naruszenia bezpieczeństwa komputerowego*.

6) od chwili wystąpienia Incydentu należy natychmiast rozpocząć rejestrowanie wszystkich faktów dotyczących jego wystąpienia Incydentu.

7) każde podjęte działanie od momentu wykrycia Incydentu do jego ostatecznego rozwiązania powinno być udokumentowane i opatrzone datą;

8) każdy dokument dotyczący Incydentu powinien być opatrzony datą i podpisany przez osobę zajmującą się Incydentem;

9) dokumentacja dotycząca Incydentów musi umożliwiać przeprowadzenie audytu lub kontroli procesu.

10) Zespół ds. ZBI sporządza Raport z każdego Incydentu. Raport jest opracowywany przez poszczególnych członków Zespołu ds. ZBI, zgodnie z ich właściwością. Wzór ***Raportu z Incydentu*** stanowi załącznik nr 3 do niniejszej procedury. Raport z Incydentu może obejmować zbiorczo większą liczbę Incydentów za określony odcinek czasu.

11) Zespół ds. ZBI każdorazowo przedkłada ***Raport z Incydentu*** do wglądu Dyrektorowi Generalnemu GDOŚ.

12) ***Raport z Incydentu*** dotyczący danych osobowych jest przedkładany przez IOD do ADO. ADO na podstawie danych wskazanych w raporcie dokonuje oceny czy odnotowane naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, których dane

zostały naruszone, ocenia rozmiar tego ryzyka i podejmuje decyzje o zgłoszeniu Incydentu Urzędowi Ochrony Danych Osobowych.

6. W ramach etapu **Powstrzymywanie, Eliminacja i odzyskiwanie** działania podejmowane są zgodnie z poniższymi wytycznymi:
   1) dobór działań i środków reagowania na przypadki naruszenia bezpieczeństwa informacji musi być adekwatny do zagrożenia dla działalności operacyjnej GDOŚ i potencjalnych strat;
   2) administratorzy systemów, serwerów, sieci lub pracownicy WI podejmują działania zmierzające do usunięcia przyczyn i skutku powstałego Incydentu;
   3) po Incydencie następuje przywrócenie systemów dotkniętych Incydentem do stanu gotowości operacyjnej. Administratorzy systemów przywracają systemy do normalnego działania, potwierdzają, że systemy działają normalnie i usuwają luki w zabezpieczeniach, aby zapobiec podobnym Incydentom. Odtwarzanie może obejmować takie działania, jak przywracanie systemów z czystych kopii zapasowych, odbudowywanie systemów od podstaw, zastępowanie zainfekowanych plików czystymi wersjami, instalowanie poprawek, zmiana haseł i zwiększanie bezpieczeństwa granic sieci (np. reguły firewalli, listy kontroli dostępu routera brzegowego). Wyższe poziomy logowania w systemie lub monitorowania sieci mogą być częścią procesu odtwarzania.;
   4) należy sprawdzić czy zainfekowane systemy funkcjonują normalnie;
   5) w razie potrzeby, należy zastosować dodatkowy monitoring w celu poszukiwania powiązanych przyszłych aktywności.
7. W ramach etapu **Działania po Incydencie** podejmowane są czynności zgodnie z poniższymi wytycznymi:
   1) po wystąpieniu Incydentu Zespół ds. ZBI organizuje spotkanie z wszystkimi podmiotami, których dotyczył Incydent. Spotkanie powinno odbyć się nie później niż w ciągu 5 dni roboczych od zakończenia Incydentu. Na spotkaniu Zespół ds. ZBI omawia Incydent dokonując analizy zdarzenia oraz działań podjętych podczas interwencji w szczególności ustalając:
      a) co się dokładnie wydarzyło i w jakim czasie?,
      b) jak skutecznie Pracownicy oraz inne osoby poradzili sobie z Incydentem? Czy przestrzegano udokumentowanych procedur? Czy były one odpowiednie?,
      c) jakie informacje były potrzebne wcześniej, przed wystąpieniem Incydentu?,
      d) czy wykonano jakieś kroki lub działania, które mogły utrudnić odtworzenie?,
      e) co personel i kierownictwo zrobiliby inaczej, gdyby następnym razem wystąpił podobny Incydent?,
      f) w jaki sposób można ulepszyć wymianę informacji z innymi organizacjami?,
      g) jakie działania naprawcze mogą zapobiec podobnym Incydentom w przyszłości?,
      h) na jakie zwiastuny lub wskaźniki należy zwrócić uwagę w przyszłości, aby wykryć podobne Incydenty?,
      i) jakie dodatkowe narzędzia lub zasoby są potrzebne do wykrywania, analizowania i łagodzenia skutków przyszłych Incydentów?.
   2) Z przebiegu spotkania Zespół ds. ZBI sporządza notatkę obejmującą w szczególności wnioski i zalecenia dotyczące Incydentu.
   3) Pełnomocnik BI powinien poinformować osoby, które zgłosiły Incydent o wynikach analizy zdarzenia i zamknięciu zgłoszenia;

4) Zespół ds. ZBI powinien sporządzać okresowo zestawienie informacji zarządczych dotyczących Incydentów dla Dyrektora Generalnego GDOŚ;

5) Ze względu na zmieniający się charakter technologii informacyjnej i zmiany personalne, Zespół ds. ZBI powinien przeglądać całą dokumentację i procedury obsługi Incydentów w wyznaczonych odstępach czasu, jednak nie rzadziej niż co 12 miesięcy, a ponadto po każdym poważnym Incydencie. W wyniku Incydentu może zajść potrzeba aktualizacji procedury reagowania na Incydenty lub innych dokumentów SZBI. Za aktualizację dokumentacji odpowiada Pełnomocnik ds. BI.

## § 6. Dokumenty związane

1) PBI Polityka Bezpieczeństwa Informacji GDOŚ.
2) Zasady bezpieczeństwa informacji w relacjach z dostawcami.

## § 7. Załączniki

1) Załącznik nr 1 – Wzór rejestru Incydentów bezpieczeństwa informacji.
2) Załącznik nr 2 – Wzór rejestru naruszeń ochrony danych osobowych.
3) Załącznik nr 3 – Wzór raportu z Incydentu.

| L.P. | Zgłaszający (imię i nazwisko) | Właściciel aktywa informacyjnego związanego z incydentem | Adres e-mail na który przysła wiadomość | Lokalizacja zdarzenia | Data otrzymania zgłoszenia | Realizujący | Przyczyna incydentu | Skutki incydentu - ich wpływ na zadania publiczne | Podjęte działania | Data zgłoszenia do CSIRT | Odpowiedź od CSIRT | Status zgłoszenia |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | | | | | | | | | | | | |
| 2. | | | | | | | | | | | | |
| 3. | | | | | | | | | | | | |
| 4. | | | | | | | | | | | | |
| 5. | | | | | | | | | | | | |
| 6. | | | | | | | | | | | | |
| 7. | | | | | | | | | | | | |
| 8. | | | | | | | | | | | | |
| 9. | | | | | | | | | | | | |

| Lp. | Wewnętrzny nr porądkowy naruszenia ochrony danych osobowych. | Data zgłoszenia naruszenia (zdarzenia). | Data naruszenia (zdarzenia). | Imię, nazwisko, stanowisko służbowe lub dane kontaktowe osoby zgłaszającej. | Zwięzły opis naruszenia (zdarzenia). | Ilość i kategoria osób, których dotyczy naruszenie. | Opis podjętych działań zaradczych. | informacja o zgłoszeniu naruszenia do właściwego organu nadzorczego. | Informacje o zawiadomieniu osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych. | Inne informacje związane z naruszeniem (zdarzeniem). |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. | | | | | | | | | | |
| 2. | | | | | | | | | | |
| 3. | | | | | | | | | | |
| 4. | | | | | | | | | | |
| 5. | | | | | | | | | | |
| 6. | | | | | | | | | | |
| 7. | | | | | | | | | | |
| 8. | | | | | | | | | | |
| 9. | | | | | | | | | | |
| 10. | | | | | | | | | | |

# *Załącznik nr 3 do Procedury zarządzania incydentami bezpieczeństwa informacji, w tym ochrony danych osobowych*

# *Wzór raportu z incydentu*

**Raport z incydentu naruszenia bezpieczeństwa informacji**

Warszawa, dnia.....

Osoba powiadamiająca o zaistniałym zdarzeniu:

…….
(Imię i Nazwisko, stanowisko służbowe, komórka organizacyjna, tel. kontaktowy, e-mail)

Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

…….
(Imię i Nazwisko, stanowisko służbowe)

Lokalizacja zdarzenia:

…….
(np. budynek, nr pokoju; nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące (np. nazwa systemu/aplikacji, którego zdarzenie dotyczy; nazwa urządzenia, w którym zaistniało zdarzenie oraz ewentualnie analogiczne informacje o innych urządzeniach objętych zdarzeniem; kiedy wystąpiło zdarzenie i czy jest powtarzalne, wstępne oszacowanie szkód, jeśli doszło do ich materializacji; czy czynnik wywołujący zdarzenie (na przykład intruz albo oprogramowanie złośliwe) został zidentyfikowany i czy jego aktywność nadal trwa?; komunikaty oraz (jeśli są dostępne) logi systemowe; ewentualne zrzuty ekranowe (w załącznikach); w przypadku gdy zdarzenie dotyczy danych osobowych, opisanie charakteru zdarzenia, w tym wskazać kogo dane osobowe (np. pracowników, interesantów) i w jakiej ilości (np. przybliżona liczba wpisów) dotyczy zdarzenie oraz czy są to dane osobowe zwykłe czy szczególnych kategorii; określenie wszelkich istotnych informacji mogących wskazywać na przyczynę zdarzenia, określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
……
……
…….

Podjęte działania:
……
……
…….

Przyczyny wystąpienia zdarzenia:
……
……
…….

Postępowanie wyjaśniające:
……
…….

Ocena skuteczności przeprowadzonych działań naprawczych:
……
……
Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobieganiu w przyszłości podobnym naruszeniom bezpieczeństwa:
……
……
…….

…….....
(data, podpis ABT)

……...
(data, podpis IOD)

……...
(data, podpis Pełnomocnika ds. BI)

**Załącznik nr 6** do Zarządzenia nr 14 Generalnego Dyrektora Ochrony Środowiska w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska z dnia 17 listopada 2022 r.

# *Procedura zarządzania ryzykiem wraz z metodyką szacowania ryzyka w Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Generalny Dyrektor Ochrony Środowiska

ANDRZEJ SZWEDA-LEWANDOWSKI

Generalny Dyrektor Ochrony Środowiska

.....

Generalny Dyrektor Ochrony Środowiska

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego Pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem niniejszej procedury jest ustanowienie zasad identyfikacji i klasyfikacji aktywów informacyjnych Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ", oraz szacowania ryzyka w bezpieczeństwie informacji.

## § 2. Zakres

Niniejszy dokument obejmuje zasadami wszystkie aktywa informacyjne GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;

2) **Analizie ryzyka** – należy przez to rozumieć proces dążący do poznania charakteru ryzyka i określenia prawdopodobieństwa wystąpienia oraz możliwego wpływu uprzednio zidentyfikowanego ryzyka;

3) **Ciągłości działania** – należy przez to rozumieć przeciwdziałanie przerwom w działalności GDOŚ oraz ochronę krytycznych procesów przetwarzania aktywów informacyjnych przed rozległymi awariami systemów informacyjnych lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie. Ogół działań wykonywanych przed, w trakcie i po awarii lub katastrofie w celu utrzymania realizacji zadań GDOŚ.

4) **Danych o stanie zdrowia** – należy przez to rozumieć dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie zdrowia. (np. informacja o korzystaniu z lub leczeniu w poradni zdrowia psychicznego);

5) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

6) **Dostępności** – należy przez to rozumieć właściwość bezpieczeństwa aktywa oznaczający dostępność informacji dla osób uprawnionych wtedy, gdy jest to niezbędne dla potrzeb ich przetwarzania, właściwość aktywa do bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;

7) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 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), którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych

umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

8) **Integralności** – należy przez to rozumieć atrybut bezpieczeństwa aktywa i zasobu informacyjnego określający jakość informacji w aspekcie kompletności, spójności i wiarygodności danych;

9) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;

10) **Nośniku danych** – należy przez to rozumieć urządzenie, papier lub inny nośnik, na którym zapisuje się i przechowuje informacje;

11) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;

12) **Postępowaniu z ryzykiem** – należy przez to rozumieć proces modyfikowania ryzyka, który powinien uwzględniać: unikanie ryzyka poprzez decyzję o nierozpoczynaniu działań powodujących ryzyko, podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy, usunięcie źródła ryzyka, zmianę prawdopodobieństwa, zmianę skutków, dzielenie ryzyka wraz z inną stroną lub stronami, zachowanie ryzyka na podstawie świadomej decyzji;

13) **Poufności** – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

14) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);

15) **ryzyku** – należy przez to rozumieć ryzyko związane z bezpieczeństwem informacji, potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów w celu spowodowania szkody (strat) dla organizacji; wartość zależna od kombinacji poziomu potencjalnych strat oraz prawdopodobieństwa wystąpienia zagrożenia;

16) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ.

## § 4. .Odpowiedzialność i uprawnienia

1. Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**
2. KKO pełnią rolę Właścicieli Aktywów informacyjnych, zwanych dalej **„WA”**, i udzielają niezbędnych informacji o nich Pełnomocnikowi ds. BI, w zakresie niezbędnym do opisania ich zawartości merytorycznej oraz innych cech niezbędnych do przeprowadzenia czynności wynikających z SZBI.
3. Dyrektor Generalny GDOŚ zatwierdza:
   1) ***Wykaz aktywów informacyjnych***;
   2) ***Rejestr ryzyka***;
   3) Postępowanie z ryzykiem i właścicieli ryzyka określone w ***Raporcie z szacowania ryzyka*** oraz innych dokumentach związanych z SZBI.
4. Właściciel ryzyka, zwany dalej **„WR”** jest odpowiedzialny za wdrożenie planów postępowania z ryzykiem.


## § 5. Proces zarządzania z ryzykiem

1. W GDOŚ Postępowanie z ryzykiem polega na wdrożeniu adekwatnych zabezpieczeń do oszacowanego ryzyka.
2. Proces zarządzania ryzykiem zgodnie z normą ISO/IEC 27005 składa się z poniższych kroków:

## § 6. Identyfikacja Aktywów informacyjnych

1. WA identyfikuje Aktywa informacyjne zgodnie ze swoim zakresem odpowiedzialności.
2. WA identyfikację Aktywów informacyjnych wykonuje zgodnie z poleceniami Pełnomocnika ds. BI, w szczególności za pomocą wskazanych przez niego narzędzi informatycznych.
3. WA podczas identyfikacji Aktywów informacyjnych uwzględnia informacje niezbędne do realizacji zadań komórki organizacyjnej, wymagania prawne wynikające z przepisów prawa powszechnie obowiązującego ustaw i rozporządzeń, a także wewnętrzne regulacje GDOŚ oraz umowy zawarte przez GDOŚ z podmiotami zewnętrznymi.
4. WA są zobowiązani do monitorowania zmian w Aktywach informacyjnych i niezwłocznego informowania Pełnomocnika ds. BI o zmianach mogących mieć wpływ na zmianę związanego z nimi ryzyka.
5. Pełnomocnik ds. BI prowadzi ***Wykaz aktywów informacyjnych*** zawierający opis Aktywów informacyjnych, ich klasę oraz wyznaczonego WA. Wzór Wykazu jest określony w Załączniku nr 1 do niniejszej procedury.
6. Dla Aktywów informacyjnych związanych z przetwarzaniem Danych osobowych podczas opracowywania i projektowania bierze się pod uwagę prawo do ochrony Danych osobowych, w szczególności zasadę domyślnej ochrony oraz ochrony w fazie projektowania.

## § 7. Klasyfikacja informacji

1. Wszystkie Aktywa informacyjne muszą być sklasyfikowane w odniesieniu do celów ochrony bezpieczeństwa informacji, a także wymogów prawnych i umownych.

2. Klasyfikacja Aktywów informacyjnych umożliwia określenie, jakie szkody wyniknęłyby dla GDOŚ w wyniku naruszenia bezpieczeństwa danego Aktywa informacyjnego.
3. Klasyfikacja Aktywów informacyjnych musi być przeprowadzona w sposób zapewniający powtarzalne wyniki.
4. Klasyfikacja Aktywów informacyjnych jest przeprowadzana przez WA. Proces klasyfikacji aktywów informacyjnych koordynuje Pełnomocnik ds. BI.
5. Klasyfikacja Aktywów informacyjnych dokonywana jest w kontekście trzech podstawowych cech bezpieczeństwa informacji:
    1) Poufności;
    2) Integralności;
    3) Dostępności.
6. WA określa wymagania dla Poufności, Integralności oraz Dostępności zgodnie z poniższymi tabelami.

| **Poziom poufności** | **Definicja (przykłady)** | **Wpływ nieautoryzowanych zmian** |
|---|---|---|
| *Bardzo wysoki* | Dane osobowe wrażliwe (art. 9 RODO).<br>Dane medyczne.<br>Dane dotyczące stanu zdrowia.<br>Informacje o ściśle ograniczonym dostępie w GDOŚ (Kierownictwo GDOŚ).<br>Akta osobowe Pracowników.<br>Informacja o przynależności związkowej. | Krytyczne negatywne skutki. |
| *Wysoki* | Dane osobowe zwykłe.<br>Informacje dostępne dla upoważnionych Pracowników. | Poważne negatywne skutki. |
| *Średni* | Informacje dostępne dla większości lub wszystkich Pracowników. | Ograniczone negatywne skutki. |
| *Niski lub brak wymagań* | Informacje dostępne dla wszystkich osób mających dostęp do pomieszczeń lub systemów teleinformatycznych GDOŚ.<br>Informacja publiczna, informacja o środowisku. | Niewielkie negatywne skutki lub ich brak. |

| **Poziom integralności** | **Definicja** | **Wpływ nieautoryzowanych zmian** |
|---|---|---|
| *Bardzo wysoki* | 100% bez błędów. | Krytyczne negatywne skutki. |
| *Wysoki* | 96-99% bez błędów. | Poważne negatywne skutki. |

| | | |
|---|---|---|
| *Średni* | 90-95% bez błędów. | Znaczący negatywny wpływ. |
| *Niski* | poniżej 90% bez błędów. | Ograniczone negatywne skutki. |

| **Poziom dostępności** | **Definicja** | **Wpływ niedostępności** |
|---|---|---|
| *Bardzo wysoki* | Dopuszczalna przerwa nie dłuższa niż 2 godziny robocze. | Krytyczne negatywne skutki. |
| *Wysoki* | Dopuszczalna przerwa nie dłuższa niż 4 godziny robocze. | Poważne negatywne skutki. |
| *Średni* | Dopuszczalna przerwa nie dłuższa niż 1 dzień roboczy. | Znaczący negatywny wpływ. |
| *Niski* | Dopuszczalna przerwa dłuższa niż 1 dzień roboczy. | Ograniczone negatywne skutki. |

7. W zależności od wybranych poziomów Poufności, Integralności oraz Dostępności, klasa Aktywa informacyjnego zależna jest od definicji podanej w tabeli poniżej. W przypadku braku możliwości dopasowania wartości Poufności, Integralności i Dostępności do odpowiedniej klasy, WA dokonuje ich korekty lub arbitralnie wybiera jedną z czterech klas, która najbardziej odpowiada Aktywu informacyjnemu będącemu przedmiotem klasyfikacji.

| **Klasa aktywa** | **Poufność** | **Integralność** | **Dostępność** |
|---|---|---|---|
| *IV* | Bardzo wysoki | Integralność lub Dostępność na poziomie: Wysoki lub Bardzo wysoki | |
| *III* | Wysoki | Integralność lub Dostępność na poziomie: Wysoki lub Bardzo wysoki | |
| *II* | Średni lub niski | Integralność lub Dostępność na poziomie: Wysoki lub Bardzo wysoki | |
| *I* | Niski | Integralność lub Dostępność na poziomie: Średni lub Niski | |

## § 8. Szacowanie ryzyka

1. WA przeprowadzają szacowanie ryzyka, na które składa się:
   1) identyfikacja ryzyka;
   2) Analiza ryzyka;
   3) ocena ryzyka.
2. Analizując ryzyka, należy uwzględnić fakt, że informacje są niematerialne. Każda informacja znajduje się w Nośniku danych. W szczególności dotyczy to przechowywania informacji w postaci elektronicznej lub

papierowej, w aplikacji lub przenoszonej/przechowywanej jako tzw. *know-how* Pracownika. Rodzaj Nośnika danych ma zasadnicze znaczenie dla oceny ryzyka i wyjaśnia, że informacje jako takie nie są objęte ochroną, a jedynie Nośnik danych, w którym się znajdują. W ten sposób Nośnik danych staje się obiektem chronionym. Ważne jest również, aby chroniony Nośnik danych, taki jak: plik, aplikacja lub serwer, nigdy niezależnie nie reprezentował wartości w sensie bezpieczeństwa informacji, ale jego wartość i poziom ochrony zależały od rodzaju przetwarzanych w nim informacji.

3. Ryzyka wynikają z zagrożenia dla Aktywa informacyjnego oraz powiązanej z nim podatności (słabości) Aktywa. Ryzyko jest kombinacją skutków oraz prawdopodobieństwa wystąpienia zdarzenia mającego wpływ na bezpieczeństwo informacji. Definicja prawdopodobieństwa wystąpienia zdarzenia oraz potencjalnych skutków dla GDOŚ przedstawiają tabele poniżej.

| **Prawdopodobieństwo wystąpienia zdarzenia** | | |
|---|---|---|
| **Poziom** | **Wartość** | **Opis** |
| Bardzo rzadko | 0 | Zdarzenia mogą być w dużej mierze wykluczone według ludzkiego uznania / występują średnio raz na dekadę lub rzadziej. |
| Rzadko | 1 | Średnio zdarzenia występują co roku. |
| Sporadycznie | 2 | Zdarzenie występuje średnio raz w miesiącu. |
| Często | 3 | Zdarzenie występuje średnio raz w tygodniu. |
| Bardzo często | 4 | Średnio zdarzenie występuje codziennie. |

| **Skutki wystąpienia zdarzenia** | | |
|---|---|---|
| **Poziom** | **Wartość** | **Opis** |
| Niski | 1 | Naruszenie bezpieczeństwa nie rodzi praktycznie żadnych skutków dla GDOŚ. |
| Średni | 2 | Naruszone jest bezpieczeństwo Aktywa informacyjnego w odniesieniu do Poufności, Integralności lub Dostępności, jednak nie rodzi ono konsekwencji prawnych, wizerunkowych i innych poważnych skutków dla GDOŚ. |
| Wysoki | 3 | W wyniku naruszenia bezpieczeństwa Aktywa informacyjnego w odniesieniu do Poufności, Integralności lub Dostępności, poważnie zakłócone są procesy zależne od korzystania z Aktywa. W wyniku zadziałania zagrożenia, GDOŚ odczuwa poważne zakłócenie natury technicznej oraz organizacyjnej. |
| Bardzo wysoki | 4 | Bardzo poważne naruszenie bezpieczeństwa Aktywa informacyjnego w odniesieniu do Poufności, Integralności lub Dostępności, które może rodzić konsekwencje prawne, wizerunkowe oraz dla Ciągłości |

| | | |
|---|---|---|
| | | działania. |

4. Dla zdarzeń związanych z przetwarzaniem Danych osobowych należy opisać skutki dla osób, których dane dotyczą, w wyniku naruszenia Poufności, Integralności oraz Dostępności Aktywa informacyjnego. Należy również wskazać poziom skutków zgodnie z opisem ogólnym skutków. Wartości skutków dobierane są zgodnie z poniższą tabelą.

| **Skutki wystąpienia zdarzenia dla osób fizycznych w związku z przetwarzaniem danych osobowych** | | |
|---|---|---|
| **Poziom** | **Wartość** | **Opis** |
| Niski | 1 | Osoby, których dane dotyczą, praktycznie nie odczuwają skutków. Strata czasu w wyniku wypełniania formalności, spam, ponowne użycie danych w celu marketingu bezpośredniego |
| Średni | 2 | Osoby mogą odczuwać istotne niedogodności, które są w stanie rozwiązać pomimo kilku trudności, np. utrata szansy np. zakupu, wyjazdu, Wzrost kosztów ubezpieczenia. |
| Wysoki | 3 | Osoby mogą odczuwać istotne konsekwencje, które są w stanie rozwiązać, wiążące się z wieloma trudnościami, np. utrata miejsca zamieszkania, długotrwałe zobowiązanie finansowe |
| Bardzo wysoki | 4 | Osoby mogą odczuwać istotne lub nawet nieodwracalne konsekwencje, np. utrata środków niezbędnych do życia, porwanie, długoterminowa lub całkowita utrata zdrowia. |

5. Następnie dokonywana jest ocena ryzyka zgodnie z poniższą tabelą.

| | | | Poziom skutków | | | |
|---|---|---|---|---|---|---|
| | | | Niski | Średni | Wysoki | Bardzo wysoki |
| | | | **1** | **2** | **3** | **4** |
| Prawdopodobieństwo | Bardzo często | **4** | 4 | 8 | 12 | 16 |
| | Często | **3** | 3 | 6 | 9 | 12 |
| | Sporadyczny | **2** | 2 | 4 | 6 | 8 |
| | Rzadko | **1** | 1 | 2 | 3 | 4 |

6. Szacowanie ryzyka jest przeprowadzane zgodnie z arkuszem kalkulacyjnym, którego wzór jest określony w Załączniku nr 2 do niniejszej procedury.
7. WR jest wskazywany przez WA, przy czym może nim być WA lub inny Pracownik. Pełnomocnik ds. BI weryfikuje wskazanie WR i jest uprawniony do jego zmiany.
8. Wartości ryzyka oraz sposób Postępowania z ryzykiem są konsultowane z Pełnomocnikiem ds. BI.
9. IOD jest odpowiedzialny za konsultacje oceny ryzyka związanego z przetwarzaniem Danych osobowych.
10. Po przeprowadzeniu czynności wskazanych w powyższych paragrafach Pełnomocnik ds. BI przygotowuje ***Rejestr ryzyka***, i przekazuje go do zatwierdzenia Dyrektorowi Generalnemu GDOŚ.

## § 9. Postępowanie z ryzykiem

1. WR jest odpowiedzialny:
    1) za przygotowanie planu Postępowania z ryzykiem o poziomie wysokim i bardzo wysokim - w terminie 10 dni roboczych liczonych od dnia zatwierdzenia ***Rejestru ryzyka***;
    2) za konsultację z Pełnomocnikiem ds. BI planu Postępowania z ryzykiem;
    3) za konsultację z IOD planu Postępowania z ryzykiem, jeżeli ryzyko jest związane z przetwarzaniem danych osobowych;
    4) za przedstawienie Dyrektorowi Generalnemu GDOŚ planu Postępowania z ryzykiem do zatwierdzenia.
2. Zgodnie z normą ISO/IEC 27005 należy wdrożyć Postępowanie z ryzykiem poprzez działania prowadzące do:
    1) modyfikowania ryzyka - polegające na zredukowaniu poziomu ryzyka przez taki wybór zabezpieczeń, aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko akceptowalne;
    2) zachowania ryzyka - polegające na podjęciu decyzji o zachowaniu (akceptacji) ryzyka bez podejmowania dalszych działań, na podstawie oceny ryzyka;
    3) unikania ryzyka - polegające na unikaniu działań lub warunków, które powodują powstanie określonych ryzyk;
    4) dzielenia ryzyka – polegające dzieleniu ryzyka z inną stroną, która może skutecznie zarządzać ryzykiem – decyzja dokonywana jest na podstawie oceny ryzyka.
3. Pełnomocnik ds. BI ocenia skuteczność wdrożenia działań wynikających z przyjętych planów Postępowania z ryzykiem.

## § 10. Monitorowanie ryzyka

1. WA, WR, IOD oraz Pełnomocnik ds. BI są odpowiedzialni za identyfikację zmian w ryzyku.
2. W przypadku konieczności wprowadzenia zmian w ***Rejestrze ryzyka*** WR oraz WA zgłaszają nowe ryzyko lub zmianę w istniejącym ryzyku do Pełnomocnika ds. BI. Po dokonaniu konsultacji Pełnomocnik ds. BI uwzględnia i wprowadza uzgodnione z WR oraz WA zmiany w ***Rejestrze ryzyka***.
3. Niezależnie od działań opisanych w § 10 ust. 1 i 2, Pełnomocnik ds. BI wraz z WA i WR dokonuje przeglądu ryzyka nie rzadziej niż co 12 miesięcy.

4. Pełnomocnik ds. BI przedstawia Dyrektorowi Generalnemu GDOŚ wnioski z przeglądu ryzyka podczas przeglądu SZBI.

## § 11. Załączniki

Załącznikami do niniejszej procedury są:

1) Załącznik nr 1 – Wykaz aktywów informacyjnych;
2) Załącznik nr 2 – Rejestr ryzyka.

| Nr aktywa | Nazwa aktywa | Opis aktywa | WA | Poufność | Integralność | Dostępność | Klasa |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | | | |

**Załącznik nr 1** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *POLITYKA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO*

# *Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

.....

Dyrektor Generalny

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 3.Cel

1. Celem niniejszej polityki jest ustanowienie zasad zarządzania zasobami i Systemami teleinformatycznymi GDOŚ.
2. Dokument ma zastosowanie do wszystkich informacji chronionych przechowywanych i przetwarzanych w Systemach teleinformatycznych GDOŚ.
3. Szczególne wymagania dla wykorzystywanych systemów dostarczanych jako usługa (SaaS) przez podmioty zewnętrzne zostały uwzględnione w niniejszej polityce.
4. PBT powinni stosować wszyscy pracownicy GDOŚ odpowiadający za zarządzanie Systemami teleinformatycznymi oraz nadzór nad bezpieczeństwem informacji w nim przetwarzanych.

## § 4.Terminologia

Ilekroć w niniejszej Polityce jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.
2) **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem Danych Osobowych jest Generalny Dyrektor Ochrony Środowiska, w imieniu którego zadania realizuje Dyrektor Generalny GDOŚ. W zakresie przetwarzania danych osobowych osób zatrudnionych w GDOŚ Administratorem Danych Osobowych jest Generalna Dyrekcja Ochrony Środowiska w imieniu której funkcję ADO wykonuje Dyrektor Generalny GDOŚ.
3) **Administratorze Merytorycznym Systemu (AMS)** – należy przez to rozumieć osobę wyznaczoną przez ABT i powołaną przez Dyrektora Generalnego GDOŚ do realizacji zadań związanych z obsługą danego systemu teleinformatycznego GDOŚ.
4) **Administratorze Technicznym Systemu (ATS)** – należy przez to rozumieć pracownika Wydziału Informatyki w Biurze Dyrektora Generalnego GDOŚ;
5) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;
6) **Ciągłości działania** – należy przez to rozumieć przeciwdziałanie przerwom w działalności GDOŚ oraz ochronę krytycznych procesów przetwarzania aktywów informacyjnych przed rozległymi awariami systemów informacyjnych lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie. Ogół działań wykonywanych przed, w trakcie i po awarii lub katastrofie w celu utrzymania realizacji zadań GDOŚ.
7) **CMDB** – należy przez to rozumieć bazę konfiguracji zawierająca wszystkie istotne informacje o poszczególnych elementach konfiguracji, zwanych „CI”, w tym sprzęcie i oprogramowaniu wykorzystywanych w GDOŚ.
8) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres

zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

9) **Dyrektorze Departamentu lub Biura –** należy przez to rozumieć dyrektora departamentu albo biura, jego zastępcę lub inną osobę wyznaczoną do kierowania komórką organizacyjną.

10) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 Rozporządzenia, którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

11) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;

12) **LAN** – należy przez to rozumieć Local Area Network;

13) **MAK** – należy przez to rozumieć Minimalną Akceptowalną Konfigurację stosowaną przez ATS w zakresie aktywów przydzielanych użytkownikom.

14) **Nośniku danych** – należy przez to rozumieć urządzenie, papier lub inny nośnik, na którym zapisuje się i przechowuje informacje

15) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.

16) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);

17) **Przełożonym** – należy przez to rozumieć bezpośredniego zwierzchnika;

18) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji w celu osiągnięcia celów GDOŚ;

19) **UTM** – należy przez to rozumieć wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia lub usługi;

20) **Uwierzytelnianiu** – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

21) **VLAN** – należy przez to rozumieć Virtual Local Area Network.

22) **WAF** – należy przez to rozumieć Web Application Firewall.

23) **WAN** – nalezy przez to rozumieć Wide Area Network.

24) **Wymaganiach Bezpieczeństwa Teleinformatycznego (WBT)** – należy przez to rozumieć obowiązujące w GDOŚ zasady i procedury, a także zgodne z obecnym stanem wiedzy oraz techniki i wytycznymi producentów sprzętu oraz oprogramowania kwestie dotyczące bezpieczeństwa teleinformatycznego;

## § 3.Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej polityki został określony w **Polityce Bezpieczeństwa Informacji.**

## § 4.Zarządzanie Aktywami Informacyjnymi

1. W GDOŚ prowadzona jest CMDB.
2. Za nadzór nad utrzymywaniem CMDB odpowiedzialny jest NWI.
3. CMDB podlega przeglądowi dokonywanemu przez NWI w regularnych odstępach czasu, nie rzadziej niż co 12 miesięcy
4. CMDB zapewnia poniższy zakres informacji o konfiguracji oraz zasobach Systemów teleinformatycznych w GDOŚ:
    1) wykaz sprzętu wraz z powiązanymi licencjami na oprogramowanie;
    2) wykaz urządzeń sieciowych;
    3) wykaz sprzętu wspomagającego takiego jak UPS, agregaty;
    4) wykaz posiadanego oprogramowania wraz z licencjami;
    5) wykaz Systemów teleinformatycznych wraz ze wskazaniem klasy systemu, AMS oraz ATS;
    6) rejestr sprzętu dotyczący stacji roboczych, laptopów, smartfonów, tabletów z przypisanym użytkownikiem (zawierający co najmniej: rodzaj urządzenia, numer seryjny, datę przekazania do użytkowania, data zwrotu), podpisy Pracownika potwierdzające odbiór i zdanie).
5. Przydzielanie Aktywów Informacyjnych użytkownikom, w szczególności sprzętu wraz z oprogramowaniem, jest wykonywane na podstawie wniosku KKO.
6. Przed wydaniem użytkownikowi ATS dostosowuje sprzęt i oprogramowanie użytkownika do WBT. ATS stosuje MAK Aktywów Informacyjnych przydzielanych użytkownikom.
7. Zwrot Aktywów Informacyjnych odbywa się zgodnie z kartą obiegową obowiązującą w GDOŚ.
8. W przypadku postępowania z Aktywami Informacyjnymi stosuje się w szczególności poniższe zasady:
    1) Aktywa Informacyjne powinny być chronione przed nieuprawnionym dostępem;
    2) w uzasadnionych przypadkach powinny być stosowane filtry prywatyzujące w celu zachowania poufności informacji wyświetlanych na ekranie komputera;
    3) pliki powinny być przechowywane na wskazanych przez ATS zasobach Systemów teleinformatycznych;
    4) elektroniczne Nośniki danych zawierające informacje chronione powinny być przechowywane w sposób zabezpieczający przed dostępem osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi.
9. W przypadku korzystania z urządzeń mobilnych, niezależnie od stosowanych odpowiednio zasad wskazanych w ust. 8, stosuje się poniższe zasady:
    1) dostęp do informacji może być zapewniony tylko po podpisaniu przez użytkowników zobowiązania do ochrony przekazanych urządzeń mobilnych;

2) urządzenie powinno umożliwiać zdalne usunięcie danych przez GDOŚ w przypadku jego kradzieży lub utraty;
3) urządzenie powinno korzystać wyłącznie z szyfrowanych połączeń bezprzewodowych;
4) o ile to możliwe, na urządzeniach mobilnych nie należy przechowywać żadnych chronionych informacji GDOŚ (klasa Aktywa informacyjnego III i IV);
5) dane na nośnikach urządzeń mobilnych powinny być zabezpieczone za pomocą szyfrowania wykorzystującego silne algorytmy kryptograficzne;
6) nadzór na urządzeniami powinien być realizowany za pomocą oprogramowania MDM (Mobile Device Management).

10. W przypadku przesyłania urządzeń lub Nośników danych zawierających informacje chronione GDOŚ stosuje się poniższe zasady:
    1) należy korzystać tylko z kurierów z weryfikacją tożsamości;
    2) opakowanie powinno być wystarczające, aby chronić zawartość przed wszelkimi fizycznymi uszkodzeniami, które mogą powstać podczas transportu, i zgodne z wszelkimi specyfikacjami producenta;
    3) należy chronić urządzenia przed wszelkimi czynnikami środowiskowymi, takimi jak narażenie na ciepło, wilgoć lub pola elektromagnetyczne;
    4) należy prowadzić logi określające zawartość Nośnika danych, zastosowane zabezpieczenia oraz rejestrować czas przekazania do przesłania i czas odbioru w miejscu docelowym.
11. W przypadku wykorzystania podpisów elektronicznych oraz certyfikatów stosuje się poniższe zasady:
    1) właściciel podpisu elektronicznego lub certyfikatu umieszczonego na zewnętrznym Nośniku danych zabezpiecza go przed dostępem osób nieupoważnionych;
    2) w przypadku uszkodzenia bądź utraty podpisu elektronicznego lub certyfikatu użytkownik niezwłocznie zawiadamia o tym fakcie Przełożonego lub właściwego KKO jednocześnie podając okoliczności zdarzenia.

## § 5.Kategorie bezpieczeństwa Systemów teleinformatycznych

1. Kategoria bezpieczeństwa Systemu teleinformatycznego, zwana dalej „KB”, zależy od wartości najwyższej klasy informacji przetwarzanych w tym systemie.
2. Stosuje się 4 kategorie bezpieczeństwa Systemu teleinformatycznego zgodnie z zasadami klasyfikacji informacji wskazanymi w ***Procedurze zarządzania ryzykiem wraz z metodyką szacowania ryzyka w Generalnej Dyrekcji Ochrony Środowiska***:
    1) Systemy teleinformatyczne o niskim wpływie – klasa informacji nie wyższa niż I;
    2) Systemy teleinformatyczne o średnim wpływie – klasa informacji nie wyższa niż II;
    3) Systemy teleinformatyczne o wysokim wpływie – klasa informacji nie wyższa niż III;
    4) Systemy teleinformatyczne o bardzo wysokim wpływie – klasa informacji IV.
3. KB uwzględnia się podczas określania minimalnych zabezpieczeń Systemów teleinformatycznych oraz dla określenia poziomu wpływu podczas szacowania ryzyka.

## § 6.Kontrola dostępu

1. W celu zapewnienia właściwego poziomu bezpieczeństwa kontrola dostępu do Aktywów Informacyjnych realizowana jest z zastosowaniem poniższych zasad:
    1) zarządzanie kontrolą dostępu – realizowane jest tylko przez upoważnionych Pracowników, mających dostęp do danych niezbędnych do wykonywanych zadań, przy zarządzaniu kontrolą dostępu stosuje się zasadę rozróżniania uprawnień dostępu;
    2) ograniczenie dostępu — przetwarzanie danych w taki sposób, aby jak najmniejsza liczba osób potrzebowała dostępu do Danych osobowych, w celu wykonywania swoich obowiązków,;
    3) ograniczenie dostępu (zawartość) — w kontekście każdej operacji przetwarzania ograniczenie dostępu tylko do tych atrybutów w zestawie danych, które są potrzebne do wykonania tej operacji;
    4) segregacja dostępu – dążenie do modelu, w którym żadna osoba nie potrzebuje pełnego dostępu do wszystkich danych w Systemie teleinformatycznym,.
2. Nadawanie uprawnień do Systemów teleinformatycznych odbywa się w GDOŚ zgodnie ***Procedurą kontroli dostępu do aktywów informacyjnych***.
3. Metody i techniki Uwierzytelnienia stosuje się w trzech warstwach dostępu do Systemu teleinformatycznego:
    1) sieci;
    2) systemu operacyjnego;
    3) aplikacji.
4. Dla Systemów teleinformatycznych o bardzo wysokim wpływie (§ 5 ust. 2 pkt 4) stosuje się dwuskładnikowe Uwierzytelnienie (2FA – 2 factor authentication) na minimum jednej z trzech warstw wskazanych w ust. 3.
5. Zasady Uwierzytelniania oraz stosowania metod i środków Uwierzytelniania, a także procedury związane z ich zarządzaniem i użytkowaniem są określone w ***Procedurach kontroli dostępu do aktywów informacyjnych***.
6. Zasady dostępu podmiotów zewnętrznych do Systemów teleinformatycznych GDOŚ regulują ***Zasady bezpieczeństwa informacji w relacjach z dostawcami***.

## § 7.Zabezpieczenia sieci teleinformatycznej

1. NWI odpowiada za:
    1) bezpieczeństwo sieci teleinformatycznej;
    2) okablowania sieci teleinformatycznej oraz okablowanie zasilające;
    3) utrzymywanie aktualnej dokumentacji sieci teleinformatycznej, okablowania sieci teleinformatycznej i okablowania zasilającego.
2. Bezpieczeństwo okablowania sieci teleinformatycznej zapewnia się poprzez:
    1) oznaczenie gniazdek i kabli w sposób umożliwiający ich identyfikację;
    2) prowadzenie okablowania sieci teleinformatycznej w sposób minimalizujący ryzyko uszkodzeń fizycznych oraz nieautoryzowanego dostępu;

3) dezaktywację niewykorzystywanych gniazdek sieci teleinformatycznej lub ich zabezpieczone za pomocą metod Uwierzytelniania urządzeń sieciowych (np. 802.1X, Port Security).

3. Bezpieczeństwo sieci wewnętrznej, zwanej dalej „LAN", zapewnia się poprzez:
   1) podział sieci na segmenty fizyczne lub logiczne np. VLAN;
   2) filtrowanie ruchu sieciowego w celu ograniczenia komunikacji pomiędzy poszczególnymi segmentami sieci wewnętrznej do zakresu niezbędnego dla wykonywania zadań przez użytkowników;
   3) kontrolowanie i ograniczenie dostępu hostów sieci wewnętrznej do Internetu oraz strefy DMZ, zwanych dalej „WAN", za pomocą stateful packet firewall;
   4) automatyczne reagowanie na zagrożenia wykryte w komunikacji sieciowej pomiędzy LAN a WAN za pomocą technologii IPS i oprogramowania antywirusowego;
   5) ograniczenie dostępu do stron WWW za pomocą mechanizmów kontroli treści tzw. content filtering i URL filtering;
   6) wydzielenie usług sieciowych GDOŚ dostępnych dla użytkowników internetowych w strefach DMZ chronionych za pomocą systemów firewall oraz IPS, a w przypadku aplikacji WWW dodatkowo za pomocą WAF;
   7) skonfigurowanie systemów firewall w taki sposób, by uniemożliwione było inicjowanie połączeń z DMZ do LAN – za wyjątkiem sytuacji, gdy inicjowana sesja sieciowa będzie dodatkowo zabezpieczana i Uwierzytelniana za pomocą technologii VPN.
4. Bezpieczeństwo sieci bezprzewodowych, zwanych dalej „WLAN", z których jest dostęp do usług sieciowych LAN, zapewnia się poprzez:
   1) stosowanie szyfrowania AES;
   2) stosowanie Uwierzytelnienia użytkownika lub urządzenia opartego o login oraz hasło np. z wykorzystaniem usługi RADIUS, OpenLDAP, Active Directory;
   3) niestosowanie protokołów i metod uznanych za obarczone znanymi podatnościami o wysokim poziomie CVSS, w szczególności TKIP oraz WEP;
   4) filtrowanie ruchu sieciowego w celu ograniczenia komunikacji pomiędzy poszczególnymi segmentami LAN i WLAN do zakresu niezbędnego dla wykonywania zadań przez użytkowników segmentów sieci bezprzewodowej;
   5) izolację segmentu WLAN dedykowanego do obsługi gości od LAN.
5. Sieć LAN posiada uruchomione mechanizmy zabezpieczające przed:
   1) niepoprawnymi konfiguracjami sieci, np. pętla na portach przełącznika sieciowego;
   2) nieautoryzowanymi serwerami DHCP;
   3) ARP cache poisoning.
6. Bezpieczeństwo plików systemowych zapewnia się poprzez:
   1) ograniczenie uprawnień użytkowników w systemach operacyjnych w taki sposób, aby tylko uprawnieni ATS wprowadzali zmiany w oprogramowaniu;
   2) stosowanie oprogramowania antywirusowego na stacjach roboczych oraz serwerach;
   3) nadzorowanie i monitorowanie prac wykonywanych przez zewnętrzne podmioty, szczególnie w Systemach teleinformatycznych oraz pomieszczeniach serwerowni.

7. W celu uzyskania właściwego poziomu bezpieczeństwa, zgodnego z obecnym stanem wiedzy i techniki, stosuje się dla systemów serwerowych:
    1) uruchomienie wyłącznie niezbędnych pakietów oprogramowania;
    2) uruchamianie wyłącznie niezbędnych usług sieciowych;
    3) instalację niezbędnych zalecanych poprawek bezpieczeństwa dla wykorzystywanego oprogramowania;
    4) skonfigurowanie polityki haseł i blokowania kont administracyjnych;
    5) skonfigurowanie dla ATS kont z ograniczonym dostępem w taki sposób, aby do wykonywania operacji wymagających wyższych uprawnień korzystali z mechanizmów czasowo podwyższających uprawnienia użytkownika, np. sudo, runas.
8. Dla wszystkich Systemów teleinformatycznych GDOŚ stosuje się ten sam redundantny wzorzec czasu z wykorzystaniem protokołu NTP/SNTP.

## § 8.Zarządzanie bezpieczeństwem Systemu teleinformatycznego

1. W GDOŚ stosuje się kontrolę fizyczną i logiczną dostępu do portów diagnostycznych i konfiguracyjnych. Zarządzanie urządzeniami sieciowymi odbywa się w sieci LAN wyłącznie z dedykowanego segmentu sieci, dostępnego wyłącznie dla upoważnionych Pracowników, z którego w szczególności korzystają ATS.
2. Zdalne zarządzanie urządzeniami sieciowymi i serwerami odbywa się wyłącznie poprzez zaszyfrowaną komunikację.
3. Zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego w Systemach teleinformatycznych GDOŚ polega w szczególności na:
    1) dbałości o aktualizację oprogramowania;
    2) minimalizowaniu ryzyka utraty informacji w wyniku awarii;
    3) ochronie przed błędami, utratą, nieuprawnioną modyfikacją;
    4) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymagań określonych w przepisach prawa.

## § 9.Bezpieczeństwo fizyczne i środowiskowe

1. Zabezpieczenie pomieszczeń serwerowni jest realizowane zgodnie z ***Zasadami bezpieczeństwa fizycznego***.
2. W pomieszczeniu serwerowni stosowane jest monitorowanie temperatury oraz wilgotności wraz z automatycznym informowaniem o przekroczeniu wartości progowych. Za ustalenie maksymalnych wartości temperatury i wilgotności odpowiedzialny jest NWI.
3. Wszystkie systemy wspomagające, w szczególności UPS, generatory prądotwórcze i klimatyzacje, powinny przechodzić okresowe przeglądy i testy zgodnie z wytycznymi producentów. Jeśli producent nie określił częstotliwości przeglądów są one wykonywane w cyklu co 6 miesięcy.
4. Zabezpieczenia pomieszczenia serwerowni powinny obejmować co najmniej:
    1) czujniki dymu wraz z możliwością alarmowania ochrony lub Pracowników;
    2) system przeciwpożarowy gaszenia gazem zgodny z odpowiednimi normami polskimi;

3) zamykanie na klucz szaf teleinformatycznych metalowych ;
4) ograniczenie dostępu do szaf teleinformatycznych tylko do upoważnionych pracowników WI;
5) zasilanie awaryjne zapewniające podtrzymanie działania Systemów teleinformatycznych przez min. 1 godzinę licząc od momentu wystąpienia braku dostaw prądu.

## § 10.Zasady stosowania zabezpieczeń kryptograficznych

1. Miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi
2. Zabezpieczenia kryptograficzne należy stosować w szczególności:
   1) na Nośnikach danych urządzeń mobilnych;
   2) na mobilnych zewnętrznych Nośnikach danych, w szczególności na pendrive i dyskach twardych;
   3) na nośnikach kopii zapasowych;
   4) w tunelach VPN;
   5) w połączeniach z siecią WLAN;
   6) w połączeniach do usług sieciowych służących do przechowywania i przesyłania danych, w szczególności poczta elektroniczna, dyski chmurowe.
3. Rozwiązania kryptograficzne powinny wykorzystywać co najmniej jeden z następujących algorytmów:
   1) symetryczny szyfr blokowy AES o długości klucza min. 256-bit;
   2) równoważne do AES algorytmy szyfrowania, np.: Twofish, Serpent;
   3) kryptograficzne funkcje skrótu SHA-2, SHA-3, Whirlpool;
   4) asymetryczny algorytm Rivest–Shamir–Adleman – RSA;
   5) protokół wymiany kluczy Diffie-Hellmann – DH;
   6) asymetryczny algorytm Digital Signature Algorithm – DSA;
   7) asymetryczny algorytm ElGamal.

## § 11.Monitorowanie Systemów teleinformatycznych

1. Wszystkie Systemy teleinformatyczne w GDOŚ posiadają włączone logowanie zdarzeń związanych z bezpieczeństwem. Zakres rejestrowanych informacji w logach powinien być adekwatny do rodzaju Systemu teleinformatycznego, KB systemu oraz wymagań prawnych dotyczących przetwarzanych w tym systemie informacji.
2. Zarządzanie logami zdarzeń związanych z bezpieczeństwem powinno odbywać się zgodnie z następującymi zasadami:
   1) pliki, w których przechowywane są zebrane logi, podlegają archiwizacji w formie okresowej rotacji;
   2) okres przechowywania logów wynosi 2 lata od momentu ich zebrania;
   3) logi powinny być przekazywane z urządzeń sieciowych i serwerowych systemów operacyjnych do usługi kolektora logów, zapewniającego ich bezpieczeństwo przed utratą oraz nieuprawnioną modyfikacją;

4) zakres zbieranych informacji w logach jest zgodny z wytycznymi producentów sprzętu i oprogramowania i powinien obejmować:

   a) identyfikator użytkownika;

   b) datę, czas i szczegóły ważnych zdarzeń, np. rozpoczęcia i zakończenia pracy w systemie;

   c) identyfikator lub lokalizację terminala;

   d) rejestr pomyślnych i odrzuconych prób dostępu do systemu;

   e) rejestr pomyślnych i odrzuconych prób dostępu do danych i innych zasobów;

   f) zmiany konfiguracji systemu;

   g) aktywacje i dezaktywacje systemów;

   h) alarmy podniesione przez usługi bezpieczeństwa;

   i) błędy, awarie i ostrzeżenia;

   j) informacje o korzystaniu z przywilejów;

   k) informacje o korzystaniu z narzędzi systemowych i aplikacji;

   l) używane pliki wraz ze sposobem użycia;

   m) adresy sieciowe i protokoły.

3. Dla wszystkich systemów serwerowych, macierzy dyskowych oraz urządzeń sieciowych prowadzone jest monitorowanie pojemności w zakresie:

   1) obciążenia procesorów;

   2) wykorzystania pamięci operacyjnej;

   3) zajętości woluminów dyskowych;

   4) obciążenia interfejsów sieciowych.

4. Dokonywanie przeglądu logów odbywa się minimum jeden raz dziennie. Przegląd powinien być dokonywany ze wsparciem oprogramowania służącego do wstępnej selekcji i analizy zapisów w logach. Potwierdzenie wykonania przeglądu dzienników audytu jest odnotowywane w Dzienniku Administratora prowadzonym przez każdego z ATS.

5. GDOŚ prowadzi monitorowanie stanowiska komputerowego użytkownika w zakresie nienaruszającym prawa do prywatności. Podczas logowania użytkownika do komputera powinien pojawiać się komunikat informujący o fakcie prowadzenia monitorowania stanowiska komputerowego użytkownika.

## § 12.Kopie zapasowe

1. Zasady dotyczące kopii zapasowych Systemów teleinformatycznych stosowane w GDOŚ zapewniają tworzenie kopii zapasowych w zakresie niezbędnym do przywrócenia możliwości realizacji zadań przez GDOŚ po wystąpieniu incydentu fizycznego bądź technicznego.

2. Sposób i forma wykonywania kopii zapasowych pozwala na testowe oraz awaryjne odtwarzanie danych.

3. Zakres danych objętych kopiami zapasowymi wraz ze szczegółowym określeniem lokalizacji zasobu, typu Nośnika danych, miejsca jego przechowywania oraz harmonogramem wykonywania kopii zapasowych określa ***Procedura wykonywania kopii zapasowych.***

## § 13.Ciągłość działania Systemów teleinformatycznych

4. Podstawą planowania i działań operacyjnych w zakresie ciągłości jest analiza wpływu zakłóceń ciągłości działania na działalność GDOŚ oraz wyniki szacowania ryzyka. Uwzględniane są również wymagania minimalne, szczególnie w zakresie poziomu redundancji w systemach krytycznych z punktu widzenia realizacji zadań GDOŚ.
5. Minimalny poziom Redundancji dla systemów krytycznych GDOŚ oraz Systemów teleinformatycznych o KB bardzo wysokiej wynosi minimum N+1. Oznacza to zapewnienie minimum jednej jednostki rezerwowej dla krytycznych zasobów Systemu teleinformatycznego.
6. Do rodzajów krytycznych zasobów należą w szczególności :
    1) hypervisory;
    2) macierze SAN;
    3) przełączniki rdzeniowe;
    4) serwerownia główna;
    5) router brzegowy;
    6) UTM brzegowy;
    7) UPS;
    8) klimatyzacja w serwerowni.
7. Zasady zarządzania Ciągłością działania są opisane w ***Procedurze zarządzania ciągłością działania Systemów teleinformatycznych***.

## § 14.Zarządzanie zmianami

1. Proces wprowadzania zmian, obejmujący uzgodnienie wymagań w zakresie bezpieczeństwa informacji do Systemów teleinformatycznych, jest realizowany zgodnie z ***Procedurą zarządzania konfiguracją i zmianami Systemu teleinformatycznego***.
2. Szczególnym rodzajem wprowadzanej zmiany w Systemie teleinformatycznym są poprawki bezpieczeństwa. Proces wprowadzania poprawek jest realizowany zgodnie z ***Procedurą zarządzania poprawkami***.

## § 15.Rozwój Systemów teleinformatycznych

1. Wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem Systemów teleinformatycznych gwarantują utrzymanie odpowiedniego poziomu bezpieczeństwa.
2. Dla każdego Systemu teleinformatycznego stosuje się poniższe zasady:
    1) należy uwzględniać wymogi bezpieczeństwa podczas zakupu lub wytwarzania nowych systemów;
    2) podczas projektowania i opracowywania systemów, które służą do przetwarzania Danych osobowych, GDOŚ oraz podmioty przetwarzające biorą pod uwagę prawo do ochrony danych osobowych poprzez stosowanie zabezpieczeń organizacyjnych i technicznych adekwatnych do oszacowanego ryzyka dla projektowanych lub planowanych operacji przetwarzania, a w szczególności stosuje się:
        a) techniki pseudonimizacji,

b) mechanizmy szyfrowania,

c) minimalizację danych,

d) ograniczenie do niezbędnej ilości zbieranych Danych osobowych,

e) ograniczenie do niezbędnego zakresu przetwarzania danych,

f) ograniczenie do niezbędnego okresu przechowywania danych,

g) techniki zapewniające odpowiedni poziom dostępności,

h) zasady nieudostępniania Danych osobowych bez interwencji danej osoby nieokreślonej liczbie osób fizycznych;

3) należy zapewnić testowanie systemu przed dopuszczeniem użytkowników do nowego systemu;

4) należy rozdzielić środowisko rozwojowe, testowe i produkcyjne;

5) należy nadzorować dostęp do kodów źródłowych oprogramowania;

6) należy opracować standardy kodowania w procesie tworzenia oprogramowania;

7) należy opracować kryteria odbioru dla nowego systemu;

8) należy zapewnić ochronę danych testowych;

9) należy ustalić zasad współpracy i nadzoru nad dostarczanymi przez strony trzecie usługami dotyczącymi realizacji prac rozwojowych.

## § 16.Audyt Systemów teleinformatycznych

1. Audyt wewnętrzny zgodności Systemów teleinformatycznych z odpowiednimi normami oraz politykami bezpieczeństwa i przepisami prawa powszechnie obowiązującego przeprowadzany jest minimum co 12 miesięcy. W ramach audytu wewnętrznego w szczególności badana jest zgodność z:
   1) niniejszą Polityką;
   2) przepisami o ochronie Danych osobowych.
2. Audyt wewnętrzny Systemów teleinformatycznych jest prowadzony zgodnie z regulacjami wewnętrznymi GDOŚ.
3. Testy skuteczności zabezpieczeń, tzw. pentesty, są prowadzone zgodnie z poniższymi zasadami:
   1) przeprowadzany jest minimum 1 pentest w roku;
   2) pentest obejmuje wybrane obszary działania Systemów teleinformatycznych adekwatnie do ryzyka wystąpienia incydentu bezpieczeństwa informacji.
4. Testy są przeprowadzane zgodnie z metodyką Open Source Security Testing Methodology (OSSTM), Penetration Testing Methodologies and Standards (PTES), Information System Security Assessment Framework (ISSAF) lub równoważną.

## § 17.Postępowanie z Nośnikami danych

1. Wszelkiego rodzaju Nośniki danych (dyski twarde, pendrive, płyty CD/DVD, taśmy magnetyczne) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją lub zniszczeniem.

2. Nośniki danych przechowywane są do czasu ustania ich przydatności. Po tym czasie są pozbawiane danych w sposób nieodwracalny lub niszczone fizycznie, zgodnie z ***Procedurą niszczenia nośników informacji***.

**Załącznik nr 2** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura kontroli dostępu do aktywów informacyjnych Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem procedury jest ustalenie zasad kontroli dostępu do Aktywów Informacyjnych oraz ochrona przed naruszeniami bezpieczeństwa informacji przetwarzanych w GDOŚ.

## § 2. Zakres

Niniejszy dokument obejmuje wszystkie Aktywa Informacyjne GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ;

2) **Administratorze Merytorycznym Systemu (AMS)** – należy przez to rozumieć osobę wyznaczoną przez ABT i powołaną przez Dyrektora Generalnego GDOŚ do realizacji zadań związanych z obsługą danego systemu teleinformatycznego GDOŚ;

3) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;

4) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

5) **Haśle** — należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

6) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;

7) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;

8) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);

9) **Systemie teleinformatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

10) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ;

11) **Uwierzytelnianiu** – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

## § 4. Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Działania poprzedzające uzyskanie dostępu do informacji GDOŚ

1. Przed uzyskaniem dostępu do Aktywów Informacyjnych:
   1) każda osoba podpisuje zobowiązanie do zachowania poufności informacji, które będzie przetwarzać w GDOŚ;
   2) każda osoba zapoznaje się z ***Regulaminem Bezpieczeństwa Informacji obowiązującym w GDOŚ***;
   3) Pracownicy uczestniczą w szkoleniu w zakresie obowiązujących w GDOŚ zasad bezpieczeństwa informacji.
2. Zobowiązanie, o którym mowa w ust. 1 pkt 1, przechowywane jest w aktach osobowych Pracownika. Zobowiązania pozostałych osób przechowywane są przez Pracowników odpowiedzialnych za koordynacje realizacji zlecenia lub umowy zawartej z podmiotem zewnętrznym.
3. Pracownicy mogą przetwarzać Dane osobowe wyłącznie na podstawie upoważnienia do przetwarzania danych osobowych wydanego przez Generalnego Dyrektora Ochrony Środowiska. Osoby prowadzące działalność gospodarczą mogą, zależnie od wytycznych IOD, przetwarzać Dane osobowe na podstawie upoważnienia do przetwarzania danych osobowych wydanego przez Generalnego Dyrektora Ochrony Środowiska lub umowy powierzenia przetwarzania danych osobowych zawartej pomiędzy osobą prowadzącą działalność gospodarczą a GDOŚ. Pracownicy podmiotów zewnętrznych mogą przetwarzać Dane osobowe wyłącznie na podstawie umowy powierzenia przetwarzania danych osobowych z tym podmiotem.

## § 6. Nadawanie, zmiana i odbieranie uprawnień w Systemie teleinformatycznym GDOŚ

1. KKO przekazuje za pomocą systemu obiegu dokumentów odpowiednio do ABT lub właściwych AMS wniosek o nadanie lub zmianę uprawnień dla danego użytkownika Systemu teleinformatycznego GDOŚ. Nadanie uprawnień następuje po spełnieniu warunków, o których mowa w § 5.
2. ABT lub AMS weryfikują treść otrzymanego wniosku i w przypadku jego akceptacji dokonują stosownych zmian uprawnień w Systemie teleinformatycznym GDOŚ. W przypadku braku akceptacji wniosku przez ABT lub AMS, wniosek jest odsyłany do wnioskodawcy wraz z określeniem przyczyny uniemożliwiającej jego realizację.
3. Po realizacji wniosku ABT lub AMS informuje wnioskującego KKO, iż uprawnienia danego użytkownika w Systemie teleinformatycznym GDOŚ zostały nadane lub zmienione.

4. Odbieranie uprawnień odbywa się na podstawie wniosku właściwego KKO. Postanowienia ust. 1-3 stosuje się odpowiednio.
5. ABT i AMS odpowiedzialni są za archiwizację wniosków o nadanie, zmianę oraz odebranie uprawnień, zgodnie z obowiązującymi w GDOŚ regulacjami wewnętrznymi w tym zakresie.
6. ABT i AMS są uprawnieni do odebrania uprawnień użytkownika w Systemie informatycznym GDOŚ w przypadkach uzasadnionego podejrzenia naruszenia bezpieczeństwa systemu przez użytkownika.

## § 7. Użytkownicy zewnętrzni

1. Zakres uprawnień użytkowników zewnętrznych ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych do przetwarzania danych osobowych.
2. Osoby skierowane do realizacji przedmiotu umowy ze strony podmiotu zewnętrznego muszą być zapoznane z dokumentem ***Regulamin Bezpieczeństwa Informacji***.
3. Zestawienie użytkowników ze strony podmiotu zewnętrznego, którzy posiadają dostęp do informacji GDOŚ, prowadzi odpowiedni dla danego systemu ABT i AMS.

## § 8. Udzielanie dostępu do informacji przetwarzanych poza Systemem informatycznym GDOŚ

Zatwierdzony zakres zadań/obowiązków danej osoby, zawarta z nią umowa oraz wydane jej upoważnienie do przetwarzania danych osobowych powinny jednoznacznie wskazywać zakres dostępu do informacji chronionych przetwarzanych poza Systemem teleinformatycznym GDOŚ.

## § 9. Przeglądy uprawnień

1. ABT i AMS są zobowiązani, w zakresie swojej odpowiedzialności, do przeprowadzania, nie rzadziej niż co 12 miesięcy, cyklicznych, regularnych przeglądów uprawnień nadanych w Systemie teleinformatycznym GDOŚ.
2. W ramach przeglądu uprawnień, o którym mowa w ust. 1, ABT i AMS przygotowują zestawienie zawierające listy użytkowników wraz z ich uprawnieniami i przekazują je następnie do weryfikacji przez właściwych KKO.
3. KKO weryfikuje czy wskazane na liście uprawnienia użytkowników są adekwatne do zakresu ich obowiązków oraz wymagań w zakresie ochrony danych osobowych i przesyła zwrotnie do ABT lub AMS potwierdzenie w ciągu maksymalnie 5 dni roboczych.
4. W przypadku wykrycia rozbieżności przez ABT lub AMS (np. konto nie zostało dezaktywowane w odpowiednim czasie) natychmiastowo blokuje on dane konto oraz informuje o tym fakcie właściwego KKO poprzez wiadomość e-mail.

## § 10. Dostęp administracyjny

1. Wymagania dotyczące haseł administracyjnych Systemu teleinformatycznego GDOŚ:
    1) hasło składa się z minimum 12 znaków;
    2) hasło powinno składać się z czterech typów znaków, którymi są małe i wielkie litery, cyfry i znaki specjalne (np. !@#);

3) hasło nie może się powtarzać (kolejne hasła muszą być od siebie różne);
4) hasła należy przechowywać w sposób gwarantujący ich poufność;
5) w przypadku, gdy system nie umożliwia stosowania 2FA (dwuskładnikowego Uwierzytelnienia) hasło musi być zmieniane minimum co 360 dni.

2. Zabrania się tworzenia haseł na podstawie:
   1) cech i numerów osobistych (np. dat urodzenia, imion itp.);
   2) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx);
   3) identyfikatora, loginu użytkownika.
3. Hasła administracyjne przechowywane są na jednym z serwerów przez ABT w zaszyfrowanym pliku lub bazie danych oprogramowania dedykowanego do zarządzania hasłami tzw. password manager.
4. Hasła administracyjne powinny być znane wyłącznie administratorom odpowiedzialnym za dany system. Utworzone hasło administracyjne wraz z powiązanym identyfikatorem w systemie (np. root, admin, administrator) powinno być każdorazowo przekazane Dyrektorowi Generalnemu GDOŚ. W przypadku nieobecności osób o uprawnieniach administracyjnych w systemie, Dyrektor Generalny GDOŚ przekazuje hasła administracyjne osobie odpowiedzialnej za administrację systemem pod nieobecność jego administratora. Po przekazaniu ww. hasła, właściwy administrator zmienia hasło administracyjne i postępuje zgodnie z zasadami zawartymi w ust. 1 i 2.

## § 11. Zarządzanie hasłami

Wymagania dotyczące haseł oraz zasady tworzenia haseł użytkowników Systemów teleinformatycznych GDOŚ są określone w ***Regulaminie Bezpieczeństwa Informacji***.

## § 12. Dostęp zdalny

Zasady zarządzania dostępem zdalnym do informacji i zasobów GDOŚ opisane zostały w ***Regulaminie Pracy Zdalnej*.**

**Załącznik nr 3** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura niszczenia Nośników oraz przekazywania do ponownego użycia Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

.....

Dyrektor Generalny

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

## Spis treści

## § 1. Cel

Celem procedury jest ustalenie zasad niszczenia Nośników danych oraz określenie wymagań bezpieczeństwa informacji dla Nośników danych przekazywanych do ponownego użycia w Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ”.

## § 2. Zakres

Niniejszy dokument stosuje się do wszystkich informatycznych Nośników danych, wydruków komputerowych i dokumentów zawierających aktywa informacyjne GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ;
2) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
3) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;
4) **Nośniku danych** – należy przez to rozumieć urządzenie, papier lub inny nośnik, na którym zapisuje się i przechowuje informacje;
5) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;
6) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);
7) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji w celu osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Niszczenie Nośników

1. W przypadku uszkodzenia lub awarii Nośnika danych i konieczności przeznaczenia go do likwidacji, GDOŚ niszczy taki Nośnik danych za pomocą metod adekwatnych do klasy informacji zapisanym na tym Nośniku danych.
2. Metody niszczenia Nośników danych powinny być zgodne z normą ISO/IEC 21964-2 lub DIN 66399.
3. Elektroniczne Nośniki danych komputerów oraz serwerów niszczy się fizycznie, a sposób niszczenia powinien zapewniać poziom minimum 4 zgodnie z powyżej podanymi normami, w szczególności:
   1) H-4 – oznacza Nośnik danych połamany na kilka kawałków i zdeformowany, gdzie wielkość elementów ≤ 2 000 mm2, a 10% materiału może przekraczać określoną wielkość, ale nie może przekraczać 3 800 mm2;
   2) E-4 – oznacza Nośnik danych (chip) połamany na kawałki i wielkość elementów ≤ 30 mm2, a 10% materiału może przekraczać określoną wielkość, ale nie może przekraczać 90 mm2;
4. Każde niszczenie Nośników danych, o których mowa w ust. 3:
   1) jest nadzorowane przez osobę upoważnioną przez Dyrektora GDOŚ;
   2) potwierdzane jest protokołem zawierającym dane identyfikujące zniszczone Nośniki danych, datę dokonania zniszczenia oraz osobę, która tego dokonała.
5. Kartki papieru niszczy się fizycznie, a sposób niszczenia powinien zapewniać poziom minimum 4 zgodnie z powyżej podanymi normami, w szczególności P-4, który oznacza szerokość ścinki papieru ≤ 6 mm, a 10% materiału może przekraczać określoną wielkość, ale nie może przekraczać 480 mm2.
6. W przypadku wykonywania przez podmiot zewnętrzny niszczenia Nośników danych zawierających Dane osobowe, osoba odpowiedzialna za organizację procesu niszczenia w GDOŚ zapewnia wcześniejsze:
   1) zawarcie umowy powierzenia przetwarzania Danych osobowych z podmiotem odpowiedzialnym za niszczenie;
   2) zobowiązanie podmiotu zewnętrznego do zachowania poufności niszczonych informacji.

## § 6. Przekazywanie do ponownego użycia

1. W przypadku przekazywania informatycznych Nośników danych do wykorzystania przez innego Pracownika, ABT zapewnia usunięcie danych za pomocą dostępnych narzędzi.
2. W przypadku przekazywania informatycznych Nośników danych poza GDOŚ (p.. firmom lub instytucjom), ABT zapewnia usunięcie danych z wykorzystaniem algorytmów niszczenia danych o skuteczności adekwatnej do klasy informacji znajdujących się na Nośnikach danych.
3. Usunięcie danych, o którym mowa w ust. 2, powinno być realizowane przy zastosowaniu jednego z poniższych algorytmów:
   1) Departament Obrony USA 5220.22-M;
   2) NAVSO P-5239-26 (RLL);

3) NAVSO P-5239-26 (MFM);
4) VSITR;
5) algorytm Petera Gutmanna;
6) algorytm Bruce'a Schneiera.

4. W przypadku konieczności przekazania informatycznych Nośników danych do serwisu, ABT przed ich przekazaniem usuwa dane lub w przypadku komputerów i serwerów usuwa dyski twarde i inne Nośniki danych zawierające aktywa informacyjne GDOŚ.
5. GDOŚ zapewnia, że umowy serwisowe i gwarancyjne na sprzęt serwerowy oraz komputerowy zapewniają wykonanie naprawy przez serwis bez konieczności przekazywania dysków twardych zawierających aktywa informacyjne GDOŚ.

**Załącznik nr 4** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura pomiaru i oceny skuteczności zabezpieczeń Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem procedury jest ustalenie zasad monitorowania skuteczności zabezpieczeń w Systemie Zarządzania Bezpieczeństwem Informacji Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ".

## § 2. Zakres

Niniejszy dokument dotyczy monitorowania zabezpieczeń aktywów informacyjnych GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.

2) **Administratorze Merytorycznym Systemu (AMS)** – należy przez to rozumieć osobę wyznaczoną przez ABT i powołaną przez Dyrektora Generalnego GDOŚ do realizacji zadań związanych z obsługą danego systemu teleinformatycznego GDOŚ;

3) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań

4) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 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), którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

5) **Kierowniku Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych

6) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;

7) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.).

8) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez

organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

1. Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**
2. IOD, ABT, AMS oraz KKO odpowiedzialni są za dostarczanie informacji niezbędnych do prawidłowej realizacji zapisów niniejszej procedury przez Pełnomocnika ds. BI.

## § 5. Pomiar i ocena skuteczności zabezpieczeń

1. W ramach procesu monitorowania skuteczności wdrożonego w GDOŚ SZBI, należy mierzyć osiąganie celów SZBI oraz skuteczność stosowanych zabezpieczeń dla aktywów informacyjnych. W szczególności należy monitorować poniższe mierniki: liczone po każdym półroczu kalendarzowym:
   1) liczba incydentów bezpieczeństwa informacji, w tym naruszeń ochrony Danych osobowych;
   2) liczba zrealizowanych przeglądów SZBI w zakresie zgodnym z pkt 9 ISO/IEC 27001;
   3) liczba zrealizowanych przeglądów dokumentacji SZBI;
   4) liczba Pracowników, którzy zostali przeszkoleni w zakresie zasad bezpieczeństwa informacji obowiązujących w GDOŚ;
   5) liczba osób, którzy nie podpisali oświadczenia o zachowaniu poufności;
   6) liczba nieudanych odtworzeń kopii zapasowych;
   7) liczba przeprowadzonych testów planów DRP i ISCP;
   8) czas pracy systemu teleinformatycznego GDOŚ bez zakłóceń ciągłości działania;
   9) liczba przeprowadzonych przeglądów uprawnień użytkowników systemów teleinformatycznych GDOŚ;
   10) liczba przeprowadzonych testów podatności systemu teleinformatycznego GDOŚ.
2. W ramach procesu monitorowania skuteczności SZBI wdrożonego w GDOŚ wykorzystywane są następujące metody monitorowania, analizy i oceny:
   1) raporty;
   2) ankiety;
   3) rejestry;
   4) przeglądy;
   5) logi systemowe.
3. Monitorowanie mierników, o którym mowa w ust. 1, odbywa się po 30 czerwca i po 31 grudnia każdego roku, w terminie nie dłuższymi niż 14 dni.
4. Wszystkie wymienione w ust. 1 mierniki weryfikowane są przez Pełnomocnika ds. BI.

5. Osoby odpowiedzialne za raportowanie wyników poszczególnych pomiarów wskaźników wymienionych w ust. 1 przedkładają informacje do Pełnomocnika ds. BI, który jest odpowiedzialny za weryfikację wartości wskaźników.
6. Podczas przeglądu SZBI Pełnomocnik ds. BI przedstawia Dyrektorowi Generalnemu GDOŚ wartości z pomiarów wykonanych od czasu ostatniego przeglądu, które są analizowane i oceniane.
7. Zestawienie monitorowanych wskaźników i ich wartości dokumentuje się.

**Załącznik nr 5** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura wykonywania kopii zapasowych Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem procedury jest ustalenie zasad postępowania w procesie wykonywania kopii zapasowych w systemie teleinformatycznym oraz ochrona przed utratą danych w celu zapewnienia wznowienia działalności w wypadku awarii infrastruktury teleinformatycznej w GDOŚ. Niniejszy dokument określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

## § 2. Zakres

1. Niniejszy dokument obejmuje zasadami System teleinformatyczny GDOŚ.
2. Kopią zapasową w szczególności objęte są:
   1) systemy operacyjne w postaci obrazu systemu;
   2) maszyny wirtualne w postaci obrazu systemu;
   3) bazy danych SQL;
   4) serwery plików;
   5) konfiguracje urządzeń sieciowych (przełączniki, firewall) w postaci zapisu konfiguracji do pliku,
   6) oprogramowanie dostarczane GDOŚ w formie usługi SaaS – forma kopii zapasowej zależna od możliwości technicznych dostępnych w usłudze.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ;
2) **Administratorze Technicznym Systemu (ATS)** – należy przez to rozumieć pracownika Wydziału Informatyki w Biurze Dyrektora Generalnego GDOŚ;
3) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Wykonywanie kopii zapasowych

1. Częstotliwość oraz retencja wykonywania kopii zapasowych określona jest w ***Harmonogramie wykonywania kopii zapasowych***, który opracowywany jest w wspólnie przez ABT i ATS.
2. Kopie zapasowe wykonywane są również każdorazowo przed wprowadzeniem istotnej zmiany konfiguracyjnej (np. aktualizacja oprogramowania, zmiana ustawień systemowych).
3. Należy zapewnić stosowanie zasady 3-2-1, co oznacza minimum 3 kopie, minimum w 2 różnych miejscach, z czego minimum jedna poza siedzibą GDOŚ.
4. Należy zapewnić utrzymywanie jednocześnie co najmniej 3 kopii zapasowych/replik/egzemplarzy danych.
5. Wszystkie wykonywane w GDOŚ kopie zapasowe przechowywane są w dwóch formach.
6. Informacja o wykonaniu kopii odnotowana jest w logach systemu. Powiadomienie o prawidłowości wykonanej kopii bezpieczeństwa każdorazowo wysyłane jest z systemu na adres e-mail: admin@gdos.gov.pl.
7. Kopie zapasowe są odpowiednio oznakowane poprzez odpowiednią nazwę wskazującą na czas wykonania kopii oraz jej zawartość i datę wykonania (nazwa pliku/folderu, ewentualnie serwera lub systemu).
8. Dostęp do kopii zapasowych mają tylko ABT i ATS.
9. ABT i ATS w regularnych odstępach czasu, co najmniej raz na kwartał, dokonują kontroli wykonania kopii bezpieczeństwa oraz przeprowadzenia testów odtworzenia.

## § 6. Przechowywanie kopii zapasowych

1. Zabrania się przechowywania kopii zapasowych w tych samych pomieszczeniach, w których znajdują się wersje produkcyjne danych nimi objętymi.
2. Należy zapewnić dodatkową lokalizację przechowywania kopii zapasowych systemów krytycznych GDOŚ – inny budynek, oddalony co najmniej 1 kilometr od miejsca przechowywania kopii produkcyjnej danych.
3. Pomieszczenia, w których znajdują się kopie zapasowe, muszą być zabezpieczone przed dostępem osób nieupoważnionych. Nośniki wymienne, na których zapisane zostały kopie zapasowe, zaleca się przechowywać w szafach odpornych na wysoką temperaturę i oddziaływanie pola elektromagnetycznego. Warunki środowiskowe pomieszczeń (temperatura, wilgotność, pole magnetyczne), w których przechowuje się nośniki zawierające kopie bezpieczeństwa, muszą odpowiadać normom określonym przez producenta tych nośników.

## § 7. Testowanie kopii zapasowych

1. ABT i AST są odpowiedzialni za przeprowadzanie okresowych testów integralności danych zapisanych w wykonanych kopiach zapasowych zgodnie z opracowanym przez nich i przyjętym ***Harmonogramem testowania kopii zapasowych***.
2. Sprawdzenie poprawności zapisanych danych powinno odbywać się poprzez testowe odtworzenie danych, a ich harmonogram powinien zostać ustalony dla każdego z typów danych, dla których wykonywane są kopie zapasowe. Stosowane formy testowania kopii zapasowych to m.in.:
   1) odzysk plików systemowych, aplikacji oraz baz danych;
   2) sprawdzenie kompletności plików;

3) weryfikacja poprawnego działania funkcji systemu;

4) weryfikacja poprawności danych systemu, w szczególności ich kompletności i wiarygodności.

3. Testowanie kopii zapasowych przeprowadzane jest w środowisku testowym.

4. Fakt wykonania testu poprawności kopii zapasowej powinien być formalnie potwierdzony przez ABT lub AST w formie krótkiego raportu (np. w formie elektronicznej wiadomości e-mail), każdorazowo przekazywanego do Pełnomocnika ds. BI.

**Załącznik nr 6** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura zarządzania konfiguracją i zmianami systemu teleinformatycznego Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem niniejszej procedury jest ustanowienie zasad nadzoru nad konfiguracją urządzeń i zmianami wprowadzanymi w Systemie teleinformatycznym GDOŚ.

## § 2. Zakres

1. Procedurę należy stosować do wszystkich Systemów teleinformatycznych w GDOŚ.
2. Zasady zarządzania zmianami konfiguracją stosuje się w szczególności:
   1) podczas wprowadzania zmian w konfiguracji urządzeń sieciowych i systemów operacyjnych;
   2) podczas wprowadzania zmian w usługach oraz Systemach teleinformatycznych;
   3) podczas wprowadzania zmian w konfiguracji systemów, aplikacji i urządzeń;
   4) aktualizując systemy i aplikacje.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.
2) **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem Danych Osobowych jest Generalny Dyrektor Ochrony Środowiska, w imieniu którego zadania realizuje Dyrektor Generalny GDOŚ. W zakresie przetwarzania danych osobowych osób zatrudnionych w GDOŚ Administratorem Danych Osobowych jest Generalna Dyrekcja Ochrony Środowiska w imieniu której funkcję ADO wykonuje Dyrektor Generalny GDOŚ.
3) **Administratorze Merytorycznym Systemu (AMS)** – należy przez to rozumieć osobę wyznaczoną przez ABT i powołaną przez Dyrektora Generalnego GDOŚ do realizacji zadań związanych z obsługą danego systemu teleinformatycznego GDOŚ.
4) **Administratorze Technicznym Systemu (ATS)** – należy przez to rozumieć pracownika Wydziału Informatyki w Biurze Dyrektora Generalnego GDOŚ;
5) **Aktywach Informacyjnych** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;
6) **Ciągłości działania** – należy przez to rozumieć przeciwdziałanie przerwom w działalności GDOŚ oraz ochronę krytycznych procesów przetwarzania aktywów informacyjnych przed rozległymi awariami systemów informacyjnych lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie. Ogół działań wykonywanych przed, w trakcie i po awarii lub katastrofie w celu utrzymania realizacji zadań GDOŚ.

7) **CMDB** – należy przez to rozumieć bazę konfiguracji zawierająca wszystkie istotne informacje o poszczególnych elementach konfiguracji, zwanych „CI", w tym sprzęcie i oprogramowaniu wykorzystywanych w GDOŚ;

8) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. nick, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

9) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć inspektora ochrony danych, o którym mowa w art. 37 Rozporządzenia, którego powołuje i odwołuje Administrator Danych Osobowych, kierując się posiadanymi przez niego kwalifikacjami zawodowymi, a w szczególności posiadaną wiedzą fachową i doświadczeniem na temat prawa oraz praktyk w dziedzinie ochrony danych osobowych oraz praktycznych umiejętności do realizacji zadań określonych w art. 39 Rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.

10) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.

11) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji w celu osiągnięcia celów GDOŚ;

## § 4. Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Zarządzanie konfiguracją

1. Celem zarządzania konfiguracją jest zadbanie o to, aby konfiguracja każdego z elementów Systemu teleinformatycznego była spójna i zgodna z założeniami projektowymi, a każda zmiana konfiguracji odnotowywana.

2. W celu zapewnienia odpowiedniego poziomu zarządzania konfiguracją ATS monitoruje nadzorowany System teleinformatyczny w GDOŚ w zakresie:

   1) utrzymania i aktualizacji stanu ewidencyjnego zasobów infrastruktury (sprzętu i oprogramowania) oraz powiązań między nimi – baza konfiguracji;

   2) umożliwienia odtworzenia pierwotnej konfiguracji systemów operacyjnych;

   3) umożliwienia automatycznej i wielokrotnej instalacji systemów zgodnie z założonym standardem konfiguracji;

   4) umożliwienia wykonywania cyklicznej weryfikacji stanu zaewidencjonowanych zasobów informatycznych ze stanem faktycznym;

5) utrzymywania historii inwentaryzacji sprzętu i oprogramowania;
6) zmian w konfiguracji sprzętowej urządzeń;
7) zmian w konfiguracji programowej urządzeń;
8) zmian oprogramowania na urządzeniach sieciowych;
9) zmian wersji systemu operacyjnego oraz uzupełnień;
10) zmian wersji oprogramowania narzędziowego oraz uzupełnień;
11) zmian wersji oprogramowania użytkowego;
12) zmian danych konfiguracyjnych (w plikach, rejestrach systemowych, bazach danych);
13) wykrywania nowych urządzeń w infrastrukturze teleinformatycznej;
14) wykrywania nowego oprogramowania na monitorowanych serwerach;
15) wykrywania aktywnych usług serwera;
16) zdalnej instalacji i aktualizacji oprogramowania na serwerach;
17) informowania o obecności nieuprawnionego oprogramowania;
18) ochrony antywirusowej;
19) dostępności uzupełnień przygotowanych przez producentów oprogramowania;
20) gromadzenia i aktualizowania informacji o konfiguracji oprogramowania i urządzeń.

3. ATS w ramach nadzorowanych systemów jest odpowiedzialny za:
   1) utworzenie i aktualizację CI w CMDB;
   2) wprowadzanie i dokumentowanie zmiany w CI;
   3) przeprowadzanie, w zaplanowanych odstępach czasu, audytów zapisów przechowywanych w CMDB – zakres audytu obejmuje aktualność CMDB w stosunku do rzeczywistego stanu konfiguracji CI;
   4) zgłoszenie do właściwego kierownika komórki wykrytych niezgodności w CMDB i wprowadzenie niezbędnych działań korygujących;
   5) zabezpieczenie CMDB w zakresie kontroli dostępu oraz kopii zapasowych.

## § 6. Zasady zarządzania zmianami

1. Wprowadza się trzy rodzaje zmian: standardową, normalną oraz pilną.
2. Wyróżnia się następujące rodzaje zmian wprowadzanych w systemie teleinformatycznym GDOŚ:
   1) **zmiana standardowa** – charakteryzuje się brakiem spadku poziomu bezpieczeństwa Systemu teleinformatycznego w GDOŚ (np. wydanie stacji roboczej użytkownikowi, instalacja aplikacji o znanej konfiguracji);
   2) **zmiana normalna –** charakteryzuje się ingerencją w konfigurację Systemu teleinformatycznego w GDOŚ (np. zmiana wersji oprogramowania, zmiana konfiguracji urządzenia sieciowego aktualizacja oprogramowania w zakresie bezpieczeństwa oprogramowania, instalacja nowego urządzenia sieciowego). Zmiana może mieć wpływ na obniżenie poziomu świadczonych usług oraz bezpieczeństwo Systemu teleinformatycznego;

3) **zmiana pilna** to zmiana zainicjowana przez incydent (np. błąd krytyczny, awaria sprzętu, atak hakerski). Zmianę wykonuje się jak najszybciej w celu przywrócenia poziomu usług.

3. W przypadku zmiany standardowej:
   1) nie poddaje się jej testom;
   2) decyzję o niej podejmuje samodzielnie ATS;
   3) nie dokumentuje się jej w Dzienniku Administratora.
4. W przypadku zmiany normalnej:
   1) poddaje się ją testom;
   2) decyzję o niej podejmuje AMS w porozumieniu z NWI;
   3) dokumentuje się ją w Dzienniku Administratora.
5. W przypadku zmiany pilnej:
   1) decyzja o takiej zmianie podejmowana jest przez NWI;
   2) jest ona dokumentowana zgodnie z zapisami ***Procedury zarządzania incydentami naruszenia bezpieczeństwa informacji***;
   3) zmianę pilną mającą charakter krytyczny należy wprowadzić zapobiegawczo i bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia pracy GDOŚ.
6. Przed wprowadzeniem zmiany należy zidentyfikować ryzyka dotyczące planowanej zmiany i zapewnić możliwość bezpiecznego wycofania zmiany, w szczególności w stosownym przypadku:
   1) wykonać kopię danych systemu objętego zmianami;
   2) wykonać kopię systemu operacyjnego wraz z plikami aplikacji;
   3) zweryfikować możliwości odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń;
   4) w razie potrzeby utworzyć bądź zaktualizować instrukcje odzyskiwania systemu;
   5) w uzasadnionych przypadkach wykonać testy w wydzielonym środowisku testowym.
7. Zmiany w konfiguracji systemów, urządzeń i aplikacji zgodnie z niniejszą procedurą są wprowadzane w szczególności w przypadku:
   1) wykrycia incydentu naruszenia bezpieczeństwa;
   2) konieczności zmiany konfiguracji;
   3) konieczności instalacji poprawki lub aktualizacji oprogramowania;
   4) instalacji nowych urządzeń lub oprogramowania.
8. Poziom stosowanych zabezpieczeń podczas wprowadzania zmian do Systemów teleinformatycznych jest adekwatny do ryzyka związanego z wprowadzaną zmianami.
9. Ryzyko dla zmiany w Systemie teleinformatycznym jest oceniane zawsze przed jej wprowadzeniem. Ocena ryzyka może przyjąć formę krótkiego opisu zagrożeń, podatności oraz prawdopodobieństwa wraz ze wskazaniem planowanych zabezpieczeń.
10. Każda zmiana związana z wysokim ryzykiem utraty danych, zakłócenia Ciągłości działania i innego naruszenia wymaganego poziomu poufności, integralności lub dostępności musi zostać opisana wraz z ryzykami i proponowanymi zabezpieczeniami. Opis przesyłany jest przez osobę odpowiedzialną za wprowadzenie zmiany do ATS, który wnioskuje do KZI i ABT o akceptację wprowadzenia zmiany

w uzgodnionym terminie. Wprowadzenie zmiany o tym poziomie ryzyka dokumentuje się w Dzienniku Administratora.

11. Dla zmian opisanym w ust. 10 stosuje się ponadto następujące zasady:
    1) testowanie zmiany odbywa się w środowisku testowym;
    2) przed dopuszczeniem użytkownika do zmienionego systemu należy uzyskać pozytywny wynik weryfikacji wprowadzonej zmiany;
    3) należy zapewnić mechanizmy umożliwiające powrót do stanu systemu na wypadek negatywnego wyniku weryfikacji, o której mowa powyżej.
12. Zmiany niezwiązane z wysokim ryzykiem, o którym mowa w ust. 10, mogą być wprowadzone po akceptacji zmiany przez ATS na podstawie własnej decyzji. Zmiana tego typu musi zostać odnotowana w Dzienniku Administratora lub w sposób zautomatyzowany w logach związanych z bezpieczeństwem Systemu teleinformatycznego.
13. W przypadku gdy wskutek wprowadzonej zmiany w konfiguracji Systemu teleinformatycznego zmieniły się cechy lub atrybuty elementu konfiguracji CI utrzymywane w CMDB wprowadzona zmiana powinna zostać uwzględniona w CMDB.
14. Poprawki bezpieczeństwa są szczególnym rodzajem wprowadzanej zmiany w systemie teleinformatycznym i wprowadzane są zgodnie z zapisami ***Procedury zarządzania poprawkami***.

## § 7. Prowadzenie prac programistycznych

1. Wytworzone oprogramowanie w ramach prowadzonych prac programistycznych powinno spełniać oczekiwania użytkowników, zostać wytworzone zgodnie z zasadami prac programistycznych, odpowiednio zabezpieczone przed dostępem osób nieupoważnionych oraz zgodne z obowiązującymi przepisami prawa w tym pod względem przetwarzania Danych osobowych.
2. Prace programistyczne mogą być realizowane przez podmiot zewnętrzny, przy czym w przypadku prac wiążących się z powierzeniem przetwarzania Danych osobowych podmiotowi zewnętrznego konieczne może być zawarcie z umowy powierzenia przetwarzania danych, co należy skonsultować z IOD.
3. Wszystkie zmiany programistyczne powinny być zgłaszane do NWI, ABT i odpowiedniego ATS, wraz z określeniem zakresu zmian.
4. Planowanie zmian programistycznych należy skoordynować z procesem zarządzania zmianami.
5. Każdorazowo powinny zostać określone kryteria odbioru prac programistycznych oraz metody wdrożenia w środowisku produkcyjnym.
6. Przed przekazaniem oprogramowania do użytku, oprogramowanie przechodzi testy wewnętrzne, za których wykonanie odpowiedzialni są AMS oraz ATS.
7. Dane wykorzystywane w ramach testów są przygotowane w oparciu o możliwie zbliżone w charakterze zdarzenia oraz indeksy do sytuacji rzeczywistych. W uzasadnionych przypadkach mogą to być dane z rzeczywistych systemów (kopia danych). W ramach testów dostęp do informacji winien być chroniony za pomocą systemu uprawnień analogicznie jak w systemach produkcyjnych. Po zakończeniu testów lub gdy system testowy nie jest już wymagany dane mogą zostać usunięte.
8. W zakresie prowadzenia prac programistycznych stosowane są następujące dobre praktyki:
    1) oprogramowanie powinno być zgodne z wymaganiami określonymi przez użytkowników;

2) oprogramowanie powinno być tworzone zgodnie z ogólnymi standardami w zakresie komentowania kodu, formatowania kodu;
3) oprogramowanie powinno być tworzone z myślą o niezawodności (np. backup);
4) oprogramowanie powinno być poddane przynajmniej podstawowym testom bezpieczeństwa:
    a) dostęp autoryzowany, dostęp nieautoryzowany,
    b) dostęp z sieci wewnętrznej, z sieci zewnętrznej,
    c) logowanie akcji użytkownika,
    d) oprogramowanie tworzone w oparciu o moduły lub frameworki dostawców zewnętrznych powinno być realizowane na podstawie na bieżąco aktualizowanych wersji używanych narzędzi;
    e) oprogramowanie powinno być tworzone z myślą o optymalnym wykorzystaniu zasobów;
    f) oprogramowanie powinno być tworzone z myślą o użytkowniku końcowym w kontekście ergonomii i łatwości użytkowania.

9. W razie potrzeby stosowane jest rozdzielenie środowisk programistycznych: rozwojowych, testowych, produkcyjnych.

**Załącznik nr 7** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura zarządzania ciągłością działania systemu teleinformatycznego Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem procedury jest ustalenie zasad postępowania w procesie zarządzania ciągłością działania i przeciwdziałanie przerwom w funkcjonowaniu Systemu teleinformatycznego GDOŚ, ochrona krytycznych procesów przed rozległymi awariami lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie.

## § 2. Zakres

Niniejszy dokument obejmuje zasadami System teleinformatyczny GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ.
2) **Administratorze Technicznym Systemu (ATS)** – należy przez to rozumieć pracownika Wydziału Informatyki w Biurze Dyrektora Generalnego GDOŚ.
3) **BIA (Business Impact Analysis)** – należy przez to rozumieć analizę wpływu zakłóceń ciągłości działania systemów teleinformatycznych na funkcjonowanie GDOŚ.
4) **Ciągłości działania** – należy przez to rozumieć przeciwdziałanie przerwom w działalności GDOŚ oraz ochronę krytycznych procesów przetwarzania aktywów informacyjnych przed rozległymi awariami systemów informacyjnych lub katastrofami oraz zapewnienie wznowienia działalności w wymaganym czasie. Ogół działań wykonywanych przed, w trakcie i po awarii lub katastrofie w celu utrzymania realizacji zadań GDOŚ.
5) **DRP** – należy przez to rozumieć Plany Odtworzenia po Katastrofie
6) **ISCP** – należy przez to rozumieć Plany Awaryjne Systemów Informatycznych.
7) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.
8) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji w celu osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Analiza BIA

1. ABT i ATS wraz z Pełnomocnikiem ds. BI opracowują wspólnie BIA wraz z oceną ryzyka wystąpienia zakłóceń, która następnie podlega przeglądom nie rzadziej niż co 12 miesięcy lub w przypadku wystąpienia istotnych zmian w organizacji.
2. W procesie analizy BIA należy:
    1) określić rodzaje wpływu i kryteria oddziaływania istotne dla funkcjonowania Systemu teleinformatycznego GDOŚ;
    2) zidentyfikować systemy, aplikacje i elementy infrastruktury teleinformatycznej wykorzystywane do realizacji zadań publicznych GDOŚ;
    3) wykorzystać rodzaje wpływów i kryteria oceny wpływów w czasie wynikające z zakłócenia realizacji zadań publicznych GDOŚ;
    4) zidentyfikować ramy czasowe, w których wpływ niewznowienia działania systemów, aplikacji lub elementów infrastruktury teleinformatycznej staną się dla GDOŚ nieakceptowalne;
    5) ustalić priorytetowe działania i ramy czasowe dla wznowienia zakłóconych systemów, aplikacji lub elementów infrastruktury teleinformatycznej przy określonej minimalnej dopuszczalnej zdolności;
    6) określić zasoby niezbędne do wsparcia priorytetowych działań;
    7) określić zależności i współzależności priorytetowych działań i zasobów;
    8) zidentyfikować ryzyka zakłócenia działania systemów, aplikacji i elementów infrastruktury teleinformatycznej GDOŚ, a następnie poddać je analizie i określić czy wymagają postępowania.
3. Celem opracowania analizy BIA zaleca się wykorzystanie formularza stanowiącego ***Załącznik B do NSC 800-34 Poradnika Planowania Awaryjnego***.

## § 6. Strategia Ciągłości Działania

1. Za opracowanie Strategii Ciągłości Działania odpowiada Pełnomocnik ds. BI.
2. Dyrektor Generalny GDOŚ wdraża Strategię Ciągłości Działania w zakresie:
    1) priorytetów dla działania GDOŚ i realizowanych przez nią zadań;
    2) stabilizowania, utrzymywania, przywracania oraz odtwarzania działania wraz z zależnościami i wspierającymi działania zasobami;
    3) zarządzania incydentami (zdarzeń powodujących zakłócenia Ciągłości działania);
    4) zmniejszania wpływu zdarzeń i kontrolowanie ich wpływu na organizację poprzez:
        a) zmniejszanie prawdopodobieństwa wystąpienia zakłócenia;
        b) skracanie czasu trwania zakłócenia;
        c) ograniczenie wpływu zakłócenia na realizację zadań publicznych i funkcjonowanie GDOŚ.
3. Strategia Ciągłości Działania podlega przeglądowi Pełnomocnika ds. BI nie rzadziej niż co 12 miesięcy lub w przypadku wystąpienia istotnych zmian w organizacji, a wnioski z przeglądu przedkładane są do akceptacji Dyrektora Generalnego GDOŚ.

## § 7. Plany Odtworzenia po Katastrofie

1. DRP ma zastosowanie do poważnych, w szczególności fizycznych zakłóceń świadczenia usługi, które uniemożliwiają dostęp do podstawowej infrastruktury obiektu przez dłuższy okres. DRP jest planem skoncentrowanym na Systemie teleinformatycznym GDOŚ, mającym na celu przywrócenie działania docelowej infrastruktury systemu, aplikacji lub infrastruktury teleinformatycznej w alternatywnym miejscu po awarii. DRP może być wspierany przez plany awaryjne poszczególnych Systemów informatycznych, dotyczące odzyskiwania pojedynczych systemów, na które ma wpływ przejście do pracy w obiekcie alternatywnym. DRP usuwa tylko zakłócenia pracy przenoszonego systemu informatycznego.
2. ABT i ATS wraz z Pełnomocnikiem ds. BI opracowują wspólnie DRP. Opracowany DRP Pełnomocnik ds. BI przekazuje Dyrektorowi Generalnemu do zatwierdzenia.
3. Zatwierdzony przez Dyrektora Generalnego DRP należy testować zgodnie z przyjętym ***Harmonogramem testowania DRP i ISCP***.
4. DRP podlegają przeglądowi Pełnomocnika ds. BI nie rzadziej niż co 12 miesięcy lub w przypadku wystąpienia istotnych zmian w GDOŚ, a wnioski z przeglądu przedkładane są do akceptacji Dyrektora Generalnego GDOŚ.

## § 8. Plany Awaryjne Systemu teleinformatycznego

1. ISCP zapewnia ustanowienie procedur oceny i odzyskiwania systemu po jego awarii. ISCP zapewnia kluczowe informacje potrzebne do odzyskiwania systemu, w tym role i obowiązki, informacje o zasobach, procedury oceny sytuacji, szczegółowe procedury odzyskiwania i testowanie systemu. ISCP różni się od DRP przede wszystkim tym, że procedury planu awaryjnego systemu informatycznego mają na celu odzyskanie systemu niezależnie od lokalizacji. ISCP można aktywować w bieżącej lokalizacji systemu lub w dowolnej innej, natomiast DRP to przede wszystkim plan specyficzny dla danego miejsca, opracowany z procedurami przenoszenia operacji jednego lub więcej systemów informatycznych z uszkodzonej lub niezdatnej do wykorzystywania lokalizacji do tymczasowej lokalizacji alternatywnej. Po tym, jak DRP pomyślnie przeniesie zasoby Systemu teleinformatycznego do innej lokalizacji, każdy z systemów, którego dotyczy problem, użyje odpowiedniego ISCP w celu przywrócenia sprawności i przetestowanie systemów oraz ich produkcyjne udostępnienie.
2. Na podstawie wyników analizy BIA i oceny ryzyka naruszenia Ciągłości działania Systemu teleinformatycznego GDOŚ, ABT i ATS wraz z Pełnomocnikiem ds. BI opracowują wspólnie ISCP. Celem opracowania ISCP zaleca się wykorzystanie formularza stanowiącego ***Załącznik A do NSC 800-34 Poradnika Planowania Awaryjnego***. Opracowane ISCP Pełnomocnik ds. BI przekazuje Dyrektorowi Generalnemu do zatwierdzenia.
3. Zatwierdzone przez Dyrektora Generalnego ISCP należy testować zgodnie z przyjętym ***Harmonogramem testowania DRP i ISCP***.
4. ISCP podlegają przeglądowi Pełnomocnika ds. BI nie rzadziej niż co 12 miesięcy lub w przypadku wystąpienia istotnych zmian.

**Załącznik nr 8** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Procedura zarządzania poprawkami*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

## Spis treści

## § 1. Cel

Niniejsza procedura określa sposób i mechanizmy identyfikacji podatności systemów teleinformatycznych. Jednocześnie wskazuje zasady aktualizacji i instalacji poprawek bezpieczeństwa dla systemów i aplikacji, wskazuje odpowiedzialność za aktualizacje, a także zasady oceny wpływu poprawek i aktualizacji na ciągłość działania systemów GDOŚ.

## § 2. Zakres

Niniejszy dokument obejmuje zasadami system teleinformatyczny GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszej Procedurze jest mowa o:

1) **Administratorze Bezpieczeństwa Teleinformatycznego (ABT)** – należy przez to rozumieć osobę wyznaczoną i upoważnioną przez ADO do realizacji zadań związanych z właściwym i bezpiecznym funkcjonowaniem systemów teleinformatycznych używanych w GDOŚ;
2) **Administratorze Technicznym Systemu (ATS)** – należy przez to rozumieć pracownika Wydziału Informatyki w Biurze Dyrektora Generalnego GDOŚ;
3) **DMZ** - Demilitarized zone – należy przez to rozumieć strefę zdemilitaryzowaną bądź ograniczonego zaufania – jest to wydzielany na zaporze sieciowej obszar sieci komputerowej nienależący ani do sieci wewnętrznej, ani do sieci zewnętrznej;
4) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ;
5) **Systemie teleinformatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji w celu osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszej procedury został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Przeglądy poprawek

1. ABT i ATS są odpowiedzialni za bieżące monitorowanie możliwych aktualizacji wykorzystywanego w GDOŚ oprogramowania, jego instalację i konfigurację zgodnie z wytycznymi producenta i dostawcy oraz najlepszymi praktykami IT.
2. Przeglądy poprawek wydanych przez producentów oprogramowania i sprzętu wykonuje się w trybie tygodniowym (np. serwerowych systemów operacyjnych, stacji roboczych użytkowników, systemów w DMZ) oraz miesięcznym (dla pozostałych, niekrytycznych systemów operacyjnych i aplikacji oraz centralnych urządzeń sieciowych).
3. Po dokonaniu przeglądu ABT i ATS planują instalację aktualizacji oraz poprawek bezpieczeństwa w terminie, w którym instalacja w minimalnym stopniu zakłóci pracę użytkowników Systemów teleinformatycznych GDOŚ.

## § 6. Instalacja poprawek

1. Osoba odpowiedzialna za instalację poprawki zobowiązana jest upewnić się, czy instalacja aktualizacji nie będzie miała negatywnego wpływu na System teleinformatyczny GDOŚ oraz na dane w nim przetwarzane.
2. Zaleca się, aby instalacja poprawek przeprowadzana była poza godzinami pracy GDOŚ. W przypadku konieczności przeprowadzenia instalacji aktualizacji w godzinach pracy GODŚ należy poinformować pracowników o planowanych pracach oraz o ich terminie (tzw. okno serwisowe).
3. Przed instalacją poprawek na instancji produkcyjnej należy wykonać odpowiednie kopie zapasowe elementów Systemu teleinformatycznego GDOŚ objętych aktualizacją.
4. Za decyzję o wprowadzeniu poprawki bezpieczeństwa odpowiada ATS odpowiedzialny za system, w którym poprawka będzie wprowadzana. Wprowadzenie poprawki bezpieczeństwa odnotowywane jest w Dzienniku Administratora. Dla poprawek stosuje się ponadto zasady:
    1) poprawki bezpieczeństwa dla serwerów muszą być wykonywane poprzez wykwalifikowanego i autoryzowanego ATS;
    2) poprawki bezpieczeństwa dla serwerów należy sprawdzać nie rzadziej niż raz na 2 tygodnie;
    3) zapewnienie przywrócenia stanu maszyny wirtualnej z przed instalacji poprawki lub w przypadku takiej konieczności testowanie zmiany w środowisku testowym;
    4) pozytywny wynik weryfikacji wprowadzonej zmiany przed dopuszczeniem użytkownika do zmienionego systemu;
    5) zapewnienie mechanizmów umożliwiających powrót do stanu systemu na wypadek negatywnego wyniku weryfikacji, o której mowa powyżej;
    6) komputery stacjonarne i laptopy muszą mieć włączone automatyczne instalacje poprawek bezpieczeństwa, jednak kontrolowane przez administratorów np. za pomocą takich usług jak Windows Server Update Services (WSUS);
    7) nigdy nie instaluje się poprawek na wszystkich komputerach stacjonarnych i laptopach w jednym czasie; stosuje się sukcesywną instalację na wybranych grupach i po pozytywnym wyniku weryfikacji poprawności instalacji i działania oprogramowania kontynuuje się instalację na kolejnych komputerach stacjonarnych i laptopach.
5. Po przeprowadzonej aktualizacji osoba odpowiedzialna za jej instalację zobowiązana jest do weryfikacji, czy instancja produkcyjna działa poprawnie po aktualizacji. W przypadku wykrycia błędów osoba odpowiedzialna za instalację poprawki po konsultacji z ABT lub ATS podejmuje decyzję o dalszym sposobie postępowania.

6. Po zakończeniu procesu instalacji poprawek osoba odpowiedzialna tworzy wpis w dzienniku administratora.

## § 7. Testy podatności

1. Cykliczne testy w postaci skanów podatności systemów operacyjnych, aplikacji oraz urządzeń sieciowych prowadzone są przez ABT co najmniej raz na pół roku.
2. Co najmniej raz w roku przeprowadzane są testy penetracyjne Systemu teleinformatycznego GDOŚ, których zakres powinien być dobierany adekwatnie do występującego ryzyka dla jego elementów.

**Załącznik nr 9** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Zasady bezpieczeństwa fizycznego w Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem niniejszego dokumentu jest przedstawienie kompleksowych ram dla zabezpieczenia mienia i budynków Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ".

## § 2. Zakres

Postanowienia opisane w niniejszym dokumencie obowiązują bezterminowo na terenie wszystkich lokalizacji GDOŚ. Jeśli udział wynajmującego, innych najemców lub osób trzecich jest niezbędny do realizacji postanowień zawartych w niniejszym dokumencie, należy z nimi zawrzeć odpowiednie umowy i udokumentować je.

## § 3. Terminologia

Pojęcia używane w niniejszej procedurze oraz innych dokumentach SZBI są zdefiniowane w dokumencie jako:

1) **Administrator Bezpieczeństwa Fizycznego (ABF)** - należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze ochrony fizycznej Stref bezpieczeństwa w GDOŚ oraz odpowiada za zapewnienie bezpieczeństwa w tych strefach.
2) **Aktywa Informacyjne** – należy przez to rozumieć wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez GDOŚ, które posiadają wartość materialną lub prawną;
3) **Awaria techniczna** – należy przez to rozumieć np.: awarie wywołane pracami serwisowymi, awarie zasilania, awarie łącza internetowego;
4) **Celowe działanie** – należy przez to rozumieć np.: kradzież, wandalizm inicjowany przez źródła wewnętrzne – pracowników GDOŚ jak i osoby z zewnątrz;
5) **Dane osobowe** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji (np. adres zamieszkania), identyfikator internetowy (np. NICK, adres IP) lub jeden lub kilka specyficznych czynników określających cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby fizycznej. Informacji nie uważa się za daną osobową umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
6) **Identyfikator** — należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7) **Kierownik Komórki Organizacyjnej (KKO)** – należy przez to rozumieć Dyrektorów Departamentów, Dyrektorów Biur, a także Kierującego Zespołem do spraw Budżetu i Finansów, Audytora Wewnętrznego oraz Kierującego Stanowiskiem do spraw Ochrony Informacji Niejawnych;
8) **Komórka organizacyjna** – należy przez to rozumieć biura i departamenty lub samodzielne stanowiska GDOŚ, określone w strukturze organizacyjnej GDOŚ;
9) **Pracownik** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.);
10) **Przełożony** – należy przez to rozumieć bezpośredniego zwierzchnika;

11) **Siła wyższa** – należy przez to rozumieć zdarzenia o charakterze przypadkowym lub naturalnym, nie do uniknięcia, np.: wyładowania elektromagnetyczne, pożar, zalanie;

12) **Strefa bezpieczeństwa** – należy przez to rozumieć cały budynek lub część budynku albo wydzielone i chronione pomieszczenie lub jego część (np. serwerownia) służące do przetwarzania aktywów informacyjnych;

13) **Strefa przetwarzania danych** – należy przez to rozumieć zespół pomieszczeń w których realizuje się zadania z zakresu przetwarzania danych osobowych.

14) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

1. Zasady ujęte w niniejszym dokumencie stosują wszyscy Pracownicy i współpracownicy GDOŚ.
2. Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszych zasad został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Ogólne zasady ochrony informacji

1. W GDOŚ miejsca przetwarzania informacji muszą być zabezpieczone w sposób gwarantujący integralność, dostępność, poufność i rozliczalność przetwarzanych informacji.
2. Dla miejsc przetwarzania informacji w GDOŚ zdefiniowane są Strefy bezpieczeństwa adekwatne do klasy informacji w nich przetwarzanych.
3. Strefy bezpieczeństwa są definiowane przez ABF i zatwierdzane przed Dyrektora Generalnego GDOŚ.
4. Określone Strefy bezpieczeństwa powinny podlegać okresowemu przeglądowi nie rzadziej niż co 12 miesięcy. Przeglądu Stref bezpieczeństwa dokonuje ABF lub inna osoba wyznaczona przez Dyrektora Generalnego GDOŚ. W wyniku przeglądu aktualizuje się informacje na temat stref. Z przeprowadzonego przeglądu ABF sporządza raport, który zatwierdza Dyrektor Generalny GDOŚ.
5. Miejsca przetwarzania informacji muszą być zabezpieczone przed zdarzeniami mogącymi spowodować uszkodzenie, zniszczenie lub kradzież nośników informacji. Zastosowane środki dla miejsc przetwarzania informacji, chroniące przed dostępem osób nieupoważnionych, muszą być adekwatne do kategorii informacji przetwarzanej na nośnikach informacji zlokalizowanych w tych pomieszczeniach. W szczególności pomieszczenia te mogą być objęte mechanizmami kontroli dostępu fizycznego, oddzielone barierami ochronnymi, objęte systemem monitoringu lub nadzorowane przez pracowników ochrony.
6. Konieczność ochrony Aktywów Informacyjnych jest określana na podstawie wyników procesu zarządzania ryzykiem w bezpieczeństwie informacji oraz wymogów umownych i prawnych.
7. Obiekty i narzędzia służące zapewnieniu kontroli dostępu są serwisowane przez wykwalifikowany personel w regularnych odstępach czasu, zgodnie ze specyfikacjami producenta. Każdy serwis lub przegląd musi zostać potwierdzony protokołem wskazującym czas, datę oraz zakres prac.

## § 6. Ochrona przed wpływem i zagrożeniami zewnętrznymi

1. Dla każdej lokalizacji należy wziąć pod uwagę ewentualne zagrożenia. Zidentyfikowane zagrożenia należy ocenić w procesie zarządzania ryzykiem w bezpieczeństwie informacji w GDOŚ. Zagrożeniami są w szczególności:
    1) Siła wyższa;
    2) błędy organizacyjne – np. otwarte drzwi do pomieszczenia podczas dłuższej nieobecności umożliwiające obecność osób nieupoważnionych w Strefach bezpieczeństwa;
    3) Awarie techniczne;
    4) Celowe działanie.
2. Wymienione powyżej rodzaje zagrożeń uwzględnia się podczas szacowania ryzyka dokonywanego zgodnie z ***Procedurą zarządzania ryzykiem wraz z metodyką szacowania ryzyka w Generalnej Dyrekcji Ochrony Środowiska***.

## § 7. Strefy bezpieczeństwa

1. Dla każdej ze Stref bezpieczeństwa powinny być określone i zdefiniowane stosowne zabezpieczenia. Przykładowe zabezpieczenia to m.in.:
    1) elektroniczny system kontroli dostępu – dostęp za pomocą indywidualnej elektronicznej karty dostępu, zwanej dalej „kartą dostępu”;
    2) mechaniczna kontrola dostępu – dostęp za pomocą klucza i zamka w drzwiach;
    3) środki konstrukcyjne – np.: okna, drzwi posiadające cechy antywłamaniowe, przeciwpożarowe i przeciwdymne;
    4) czujniki detekcji – np.: czujniki ruchu, bariery świetlne, czujniki dźwięków i czujniki stłuczenia szkła, ale także czujniki dymu i ognia.
2. Strefy bezpieczeństwa muszą być nadzorowane w zależności od ich wymagań ochrony. Szczegóły wynikają z wymagań właściwej Strefy bezpieczeństwa.
3. Ze względu na różne obszary pracy i wrażliwość przetwarzanych w nich informacji, poszczególne części budynku lub obszary wymagają różnych środków ochronnych. Strefy bezpieczeństwa w miarę możliwości powinny być konstruowane koncentrycznie, tj. strefy o najwyższych wymaganiach ochrony znajdują się wewnątrz i dlatego są chronione kilkoma zewnętrznymi poziomami bezpieczeństwa. Jeżeli warstwowy model nie może być wdrożony we wszystkich obszarach, możliwe jest pominięcie stref ochronnych z uwzględnieniem ogólnych środków bezpieczeństwa (np. poprzez zintegrowanie środków ochronnych z niższych Stref bezpieczeństwa) jeżeli wyższa strefa ochrony nie definiuje właściwego odpowiednika.
4. Wymagania ochrony informacji dotyczące Stref bezpieczeństwa stosuje się odpowiednio do miejsc, które znajdują się poza obszarami własnymi GDOŚ, a mimo to przetwarzane są tam informacje będące własnością GDOŚ. Obejmuje to w szczególności systemy teleinformatyczne utrzymywane przez usługodawców (poprzez zastosowanie odpowiednich postanowień umownych), urządzenia mobilne, które Pracownicy zabierają ze sobą w podróże służbowe oraz nośniki danych.
5. Mając na uwadze ochronę Aktywów Informacyjnych, GDOŚ bierze pod uwagę przy projektowaniu Stref bezpieczeństwa fizycznego następujący model stref:

1) Strefa publiczna – Strefa 1 – Obszar o charakterze publicznym, który jest ogólnie dostępny dla wszystkich, czasowo lub na stałe. W tej strefie obowiązują podstawowe wymagania bezpieczeństwa (np. polityka czystego biurka i ekranu);
2) Strefa kontrolowana – Strefa 2 – Obszar jest dostępny tylko dla ograniczonej grupy osób. W tym obszarze przetwarzane są informacje sklasyfikowane na poziomie nie wyższym niż III. W tej strefie obowiązują następujące wymagania bezpieczeństwa:
    a) wszystkie Aktywa informacyjne należy chronić i kontrolować do nich dostęp,
    b) dostęp jest ograniczony do Pracowników i zarejestrowanych gości pod nadzorem upoważnionego Pracownika,
    c) poza godzinami pracy przebywanie w tej strefie jest dozwolone tylko po zatwierdzeniu każdorazowo przez właściwego KKO;
3) Strefa ograniczona – Strefa 3 – Obszar jest dostępny tylko dla ściśle ograniczonej grupy osób. W tych obszarach przetwarzane są informacje o poziomie klasyfikacji IV. W tej strefie obowiązują następujące wymagania bezpieczeństwa:
    a) dostęp jest ograniczony do upoważnionych Pracowników i zarejestrowanych gości pod nadzorem upoważnionego Pracownika,
    b) poza godzinami pracy dostęp do tej Strefy bezpieczeństwa jest dozwolony tylko w wyjątkowych przypadkach, dostęp musi być zatwierdzony każdorazowo przez Dyrektora Generalnego GDOŚ.

6. Postanowień ust. 1-5 nie stosuje się do pomieszczeń kancelarii tajnej.

## § 8. Pomieszczenie serwerowni

1. Serwerownia GDOŚ stanowi obszar, w którym znajdują się elementy infrastruktury teleinformatycznej (np. elementy sieci), które wymagają ochrony. Obszar ten dostępny jest tylko dla ściśle określonej grupy osób, tj. upoważnionych pracowników Wydziału Informatyki BDG i innych zarejestrowanych osób przebywających pod stałym nadzorem upoważnionego pracownika Wydziału Informatyki BDG.
2. Dostęp do serwerowni GDOŚ poza godzinami pracy jest dozwolony tylko w wyjątkowych przypadkach dla upoważnionych pracowników Wydziału Informatyki BDG, a dla pozostałych osób musi zostać każdorazowo zatwierdzony przez Dyrektora BDG.
3. Każde wejście do serwerowni GDOŚ osoby nie będącej upoważnionym Pracownikiem musi być zarejestrowane bezpośrednio przed wejściem, a osoba wchodząca powinna być pouczona o wymaganiach ochronnych obowiązujących w pomieszczeniu.
4. W serwerowni GDOŚ zabronione jest korzystanie ze sprzętu teleinformatycznego lub oprogramowania nie będącego własnością GDOŚ. Dyrektor Generalny GDOŚ, w uzasadnionych przypadkach, może wyrazić zgodę na korzystanie z takiego sprzętu lub oprogramowania po uprzednim zasięgnięciu opinii ABT.
5. Obszar serwerowni GDOŚ jest trwale chroniony przed nieuprawnionym dostępem poprzez zastosowanie środków technicznych w postaci:
    1) mechanicznego systemu blokującego dostęp;
    2) zainstalowania systemu sygnalizacji włamania, który monitoruje wszystkie obszary dostępu i dostępne wejścia.
6. Pomieszczenia serwerowni GDOŚ objęto ochroną realizowaną przez elektroniczny system antywłamaniowy z całodobowym monitoringiem sygnału alarmowego.

7. Wejście do serwerowni GDOŚ objęto całodobowym nadzorem realizowanym przez system monitoringu wizyjnego.
8. Wejście do serwerowni GDOŚ jest zabezpieczone dodatkowym kodem dostępu oraz kluczem i kartą dostępu.
9. Dostęp do serwera przechowującego dane jest ograniczony jedynie dla osób uprawnionych.

## § 9. Wykaz budynków, pomieszczeń oraz sposób i zasady ich zabezpieczeń fizycznych

1. GDOŚ funkcjonuje w dwóch lokalizacjach:
   1) ul. Wawelska 52/54, 00-922 Warszawa – budynek Ministerstwa Klimatu i Środowiska, zwanego dalej „MKiŚ", w Warszawie;
   2) Al. Jerozolimskie 136, 02-305 Warszawa – piętro 12 i 13 w budynku biurowym „Eurocentrum".
2. W celu zapewnienia bezpieczeństwa i rozliczalności dostępu do pomieszczeń biurowych, w których przetwarzane są Aktywa informacyjne w tym dane osobowe, w budynkach wykorzystywanych przez GDOŚ wprowadza się następujące zasady bezpieczeństwa, kontroli dostępu i postępowania z kluczami oraz elektronicznymi kartami dostępu:
   1) kopiowanie lub wykonanie duplikatu kluczy do pomieszczeń wymaga pisemnej zgody Dyrektora Generalnego GDOŚ i jest dozwolone wyłącznie w celu:
      a) przekazania do przechowywania i wykorzystania upoważnionemu Pracownikowi,
      b) zastąpienia kluczy utraconych, uszkodzonych lub zniszczonych;
   2) zabrania się:
      a) samodzielnego dorabiania kluczy,
      b) udostępniania osobom nieupoważnionym kluczy, kart dostępu i kodów dostępowych oraz kodów sterujących systemami alarmowymi,
      c) pozostawiania otwartych pomieszczeń lub kluczy bez dozoru,
      d) pozostawiania otwartych okien po zakończeniu pracy,
      e) wynoszenia klucza do pomieszczenia zajmowanego przez GDOŚ poza obszar budynku, w którym to pomieszczenie się znajduje,
      f) pozostawiania otwartych drzwi do powierzchni GDOŚ,
      g) wpuszczania osób nieuprawnionych do powierzchni GDOŚ;
   3) klucze zapasowe do pomieszczeń GDOŚ, w imieniu Dyrektora BDG, przechowuje Naczelnik Wydziału Organizacyjnego BDG;
   4) kluczami zapasowymi do pomieszczeń mają prawo posługiwać się wyłącznie Pracownicy wykonujący zadania służbowe, którzy zostali upoważnieni przez Dyrektora BDG, a w przypadku kluczy do pomieszczeń biurowych w Strefie ograniczonej: Kancelarii ogólnej, kancelarii tajnej, serwerowni, składu chronologicznego, biura Generalnego Dyrektora Ochrony Środowiska oraz Zastępcy Generalnego Dyrektora Ochrony Środowiska, biura Dyrektora Generalnego GDOŚ, biur KKO oraz sekretariatów poszczególnych komórek organizacyjnych GDOŚ – wyłącznie Pracownicy wykonujący zadania służbowe, którzy zostali upoważnieni przez Dyrektora Generalnego GDOŚ;

5) utratę, uszkodzenie lub zniszczenie klucza, worka lub saszetki na klucze lub indywidualnej karty dostępu, Identyfikatora, jak również naruszenie plomby na worku lub saszetce na klucze, Pracownik zgłasza poprzez przesłanie wiadomości mailowej do Dyrektora BDG za pośrednictwem Naczelnika Wydziału Organizacyjnego BDG, powiadamiając również o tym właściwego KKO;

6) jeśli zgłoszenie, o którym mowa w pkt 5, dotyczy karty dostępu, Identyfikatora lub kluczy do pomieszczeń biurowych w budynku MKiŚ, zgłoszenie takie jest przekazywane również do Biura Dyrektora Generalnego MKiŚ;

7) klucze uszkodzone lub zniszczone oraz uszkodzone lub zniszczone Identyfikatory lub indywidualne karty dostępu należy zdać Naczelnikowi Wydziału Organizacyjnego BDG celem ich zabezpieczenia i wycofania z użytkowania;

8) w przypadku otrzymania informacji o utracie klucza Identyfikatora lub indywidualnej karty dostępu Naczelnik Wydziału Organizacyjnego BDG zgłasza do Naczelnika Wydziału Informatyki BDG fakt utraty Identyfikatora lub indywidualnej karty dostępu celem zablokowania możliwości korzystania z niej, a w przypadku utraty klucza, o ile z okoliczności jego utraty wynika, że może zostać on użyty przez osobę nieupoważnioną, wymienia zamek albo niezbędne elementy zamka;

9) klucze uszkodzone lub zniszczone należy przechowywać lub usuwać w sposób uniemożliwiający wykorzystanie ich do nieuprawnionego dostępu do pomieszczeń.

3. Dostęp do szaf podlegających zabezpieczeniu i sejfów pod nieobecność upoważnionego Pracownika lub osoby go zastępującej wymaga każdorazowo pisemnej zgody Dyrektora Generalnego GDOŚ. Otwarcia tych szaf i sejfów dokonują osoby wskazane przez Dyrektora Generalnego GDOŚ.

4. Wejście do pomieszczeń GDOŚ w Strefie kontrolowanej pod nieobecność upoważnionego Pracownika lub osoby go zastępującej wymaga każdorazowo zgody właściwego KKO.

5. Po dokonaniu czynności, o których mowa w ust. 3 i 4, sporządza się protokół, którego wzór stanowi załącznik nr 1 do niniejszej procedury.

6. Po komisyjnym otwarciu pomieszczenia, sejfu lub szafy, w ramach procedury opisanej w ust. 3 i 4, i wykonaniu czynności nakazanych przez Dyrektora Generalnego GDOŚ, osoby dokonujące czynności zobowiązane są do zabezpieczenia dokumentów i materiałów pozostających w otwartych pomieszczeniach, szafach i sejfach przez zamknięcie ich na klucz, a jeśli to jest niemożliwe z przyczyn technicznych – poprzez założenie plomby zabezpieczającej.

### 1.1 Pomieszczenia biurowe i techniczne w budynku przy ul. Wawelskiej 52/54, 00-922 Warszawa

1. Rozmieszczenie pomieszczeń biurowych i technicznych w budynku przy ul. Wawelskiej 52/54, 00-922 Warszawa, w których przetwarzane są Aktywa informacyjne w tym Dane osobowe administrowane przez GDOŚ, przedstawia w formie graficznej załącznik nr 2 do niniejszej procedury.

2. Zabezpieczenie fizyczne i kontrola dostępu do Strefy przetwarzania danych realizowane są przez służby ochrony MKiŚ.

3. Zabezpieczenie fizyczne i kontrola dostępu do Strefy przetwarzania danych obejmującej wejście do korytarza na IV piętrze w części północnej budynku MKiŚ oraz wejścia do udostępnionych pomieszczeń znajdujących się w holu przywindowym na IV piętrze przy klatce schodowej E budynku MKiŚ odbywa się za pomocą indywidualnej karty dostępu, zgodnie z przyznanymi indywidualnymi uprawnieniami dostępu.

4. Pobieranie i deponowanie kluczy w recepcji MKiŚ odbywa się z wykorzystaniem depozytora kluczy, do którego dostęp jest możliwy za pomocą indywidualnej karty dostępu, na której zakodowane są indywidualne uprawnienia dostępu. System obsługi depozytora rejestruje każdorazowo pobranie i zdanie kluczy. Uprawnienia do pobierania kluczy nadaje MKiŚ.

5. Do pobierania i deponowania kluczy użytku bieżącego od pomieszczeń są upoważnieni:
   1) pracownicy znajdujący się w „Wykazie osób upoważnionych do pobrania kluczy";
   2) pracownicy zastępujący prowadzących sprawę lub postępowanie;
   3) pracownicy posiadający jednorazowe upoważnienie.
6. Wykaz osób upoważnionych do pobrania kluczy użytku bieżącego sporządza i aktualizuje Dyrektor BDG, na podstawie informacji przesyłanych e-mailem przez KKO.
7. Upoważnień jednorazowych udziela Dyrektor BDG na podstawie uzasadnionego wniosku KKO właściwego ze względu na miejsce zatrudnienia pracownika. Wniosek jest przekazywany za pośrednictwem EZD lub poczty e-mail. Wniosek i upoważnienie powinny zostać zamieszczone w systemie informatycznym wykorzystywanym do obsługi elektronicznego obiegu dokumentów w GDOŚ. Jednorazowe upoważnienie do pobrania kluczy przekazuje się do MKiŚ.
8. Wniosek o dostęp do pomieszczeń Strefy ograniczonej obejmującej w budynku przy ul. Wawelskiej 52/54 kancelarię ogólną, kancelarię tajną, serwerownię, skład chronologiczny oraz biura Generalnego Dyrektora Ochrony Środowiska oraz Zastępcy Generalnego Dyrektora Ochrony Środowiska, zatwierdza Dyrektor Generalny GDOŚ.
9. Pracownicy, goście i interesanci przebywający w budynku są zobowiązani do noszenia Identyfikatorów.
10. Niedopuszczalne jest udostępnianie Identyfikatorów innej osobie lub korzystanie z Identyfikatorów innych osób.
11. W przypadku gdy z jakichkolwiek przyczyn pracownik GDOŚ nie posiada przy sobie Identyfikatora, jest zobowiązany zgłosić ten fakt w Biurze Przepustek MKiŚ oraz pobrać Identyfikator tymczasowy, który zobowiązany jest zwrócić po zakończeniu pracy.

### 1.2 Pomieszczenia biurowe i techniczne w budynku przy Al. Jerozolimskich 136, 00-305 Warszawa,

1. Rozmieszczenie pomieszczeń biurowych i technicznych w budynku przy Al. Jerozolimskich 136, 00-305 Warszawa, w których przetwarzane są Aktywa informacyjne w tym dane osobowe administrowane przez GDOŚ, przedstawiają w formie graficznej załączniki nr 3 i 4 do niniejszego dokumentu.
2. GDOŚ zajmuje 12 i 13 piętro w budynku biurowym „Eurocentrum", przy czym:
   1) pomieszczenia zlokalizowane na piętrze 12 budynku tworzą jedną strefę administracyjną, będącą strefą pracowniczą, w której wydzielone są pomieszczenia biurowe dla pracowników GDOŚ – Strefa kontrolowana;
   2) pomieszczenia zlokalizowane na piętrze 13 budynku podzielone są na dwie strefy administracyjne:
      a) strefa pracownicza z wydzielonymi pomieszczeniami biurowymi dla pracowników GDOŚ – Strefa kontrolowana,
      b) strefa VIP (biura Dyrektora Generalnego GDOŚ oraz Dyrektora BDG GDOŚ) z wydzielonymi pomieszczeniami biurowymi, oddzielona od strefy pracowniczej dodatkowymi drzwiami z elektroniczną autoryzacją dostępu dla upoważnionych pracowników GDOŚ - Strefa ograniczona.
3. Dostęp do pięter zajmowanych przez GDOŚ, w tym do depozytora kluczy oraz wydzielonej strefy dla kluczowych pracowników GDOŚ, odbywa się za pomocą indywidualnej karty dostępu, na której zakodowano indywidualne uprawnienia dostępu dla każdego pracownika.
4. Dostęp do poszczególnych pomieszczeń zlokalizowanych w strefach administrowanych przez GDOŚ odbywa się przy wykorzystaniu kluczy pobieranych przez poszczególnych pracowników z depozytora

kluczy. Depozytor kluczy umożliwia pracownikowi pobranie kluczy na podstawie indywidualnej karty dostępu. Pobranie kluczy przez pracownika jest możliwe i ograniczone jedynie do pomieszczeń, do których uzyskał on upoważnienie i zgodnie z uprawnieniami nadanymi i zakodowanymi na indywidualnej karcie dostępu.

5. Każdorazowe pobranie i zwrot kluczy jest rejestrowane w systemie informatycznym obsługującym depozytor kluczy.
6. Nadanie uprawnień dostępu do pomieszczeń w zakresie odpowiadającym powierzonym pracownikowi obowiązkom na zajmowanym stanowisku pracy oraz wydanie indywidualnej karty dostępu dla pracownika odbywa się na podstawie wniosku KKO właściwego ze względu na miejsce zatrudnienia pracownika.
7. Uprawnienia dostępu do pomieszczeń nadawane są przez Dyrektora BDG.
8. Zabezpieczenie fizyczne i kontrola dostępu do strefy wind, parkingu i części ogólnej budynku realizowane są przez pracowników portierni oraz służby ochrony zarządcy budynku biurowego „Eurocentrum".
9. Kontrola dostępu do 12 i 13 piętra budynku przy Al. Jerozolimskie 136 (piętra zajmowane przez GDOŚ), realizowana jest przy użyciu indywidualnych kart dostępu.
10. W budynku przy Al. Jerozolimskie 136, na piętrach zajmowanych przez GDOŚ wprowadzono obowiązek noszenia przez pracowników Identyfikatorów. Niedopuszczalne jest udostępnianie Identyfikatorów innej osobie lub korzystanie z Identyfikatorów innych osób. W przypadku gdy z jakichkolwiek przyczyn pracownik GDOŚ nie będzie posiadał przy sobie Identyfikatora, jest zobowiązany zgłosić ten fakt portierowi lub pracownikowi ochrony budynku.
11. Brak Identyfikatora należy zgłaszać do Naczelnika Wydziału Organizacyjnego BDG celem wydania Identyfikatora tymczasowego, który pracownik zobowiązany jest zwrócić po zakończeniu pracy.
12. Przypadki zagubienia lub kradzieży Identyfikatorów obligatoryjnie podlegają zgłoszeniu do Dyrektora BDG GDOŚ oraz Naczelnika Wydziału Organizacyjnego BDG.
13. Dodatkowo w budynku przy Al. Jerozolimskich 136 administrator budynku wprowadził niżej wymienione zabezpieczenia:
    1) wejścia do obszarów biurowych GDOŚ na piętrze 12 i 13 są objęte monitoringiem wizyjnym;
    2) rejon holu głównego budynku oraz parking podziemny są objęte monitoringiem wizyjnym;
    3) dostęp do strefy wind, ograniczony jest bramkami otwieranymi przy użyciu kart dostępu lub przez pracowników portierni lub ochrony budynku.
14. Administratorem danych osobowych gromadzonych przez system kamer monitoringu oraz system kontroli dostępu do budynku jest właściciel budynku.

## § 10. Goście

1. Za gościa uważa się każdą osobę, która nie jest upoważnionym Pracownikiem, a także osobę realizującą dla GDOŚ zadania na podstawie umów zlecenia i innych umów cywilnoprawnych. Każdy gość wchodzący na teren GDOŚ, musi być zarejestrowany w „Księdze Gości" prowadzonej przez sekretariat Komórki organizacyjnej przyjmującej gościa. Goście mogą poruszać się po budynku i pomieszczeniach GDOŚ tylko w towarzystwie Pracownika.
2. Jeżeli do prac konserwacyjnych i naprawczych wykorzystywane są osoby niezatrudnione w GDOŚ, należy im towarzyszyć i monitorować ich pracę, aby uniknąć wypadków i zapobiec niepożądanym działaniom, w szczególności zniszczeniu lub uszkodzeniu mienia GDOŚ. Szczegóły postępowania wynikają z wymagań

właściwej Strefy bezpieczeństwa oraz zarządzeń Dyrektora Generalnego MKiŚ oraz Dyrektora Generalnego GDOŚ. Goście przebywający w danym budynku są zobowiązani do noszenia Identyfikatorów.

3. Goście w budynku **przy ul. Wawelskiej** 52/54 w Warszawie są wpuszczani do Strefy bezpieczeństwa GDOŚ jedynie po telefonicznym potwierdzeniu przez pracownika Biura Przepustek, w odpowiednim sekretariacie lub u pracownika merytorycznego, zaproszenia oraz otrzymaniu Identyfikatora z napisem „GOŚĆ". Goście mogą wejść do Strefy bezpieczeństwa administrowanej przez GDOŚ jedynie w towarzystwie pracownika komórki organizacyjnej do której się udają. Po zakończonej wizycie pracownik komórki organizacyjnej jest odpowiedzialny za odprowadzenie gości do Biura Przepustek.
4. Goście w budynku **przy Al. Jerozolimskich** 136 w Warszawie są wpuszczani do Strefy bezpieczeństwa GDOŚ jedynie po telefonicznym potwierdzeniu, w odpowiednim sekretariacie lub u pracownika merytorycznego, zaproszenia przez pracownika portierni lub ochrony budynku. Goście mogą wejść do Strefy bezpieczeństwa administrowanej przez GDOŚ jedynie w towarzystwie pracownika komórki organizacyjnej do której się udają. Przedstawiciel komórki organizacyjnej GDOŚ, jest odpowiedzialny za odprowadzenie gości do strefy wind lub holu budynku.

## § 11. Dokumenty związane

1. Polityka Bezpieczeństwa Informacji.
2. Polityka Przetwarzania Danych Osobowych.
3. Procedura kontroli dostępu do Aktywów informacyjnych.

## § 12. Załączniki

Załącznikami do niniejszej procedury są:

1) Załącznik nr 1 – Wzór protokołu komisyjnego otwarcia pomieszczenia/szafy/sejfu.
2) Załącznik nr 2 – Rzut piętra IV w budynku przy ul Wawelskiej 52/56.
3) Załącznik nr 3 – Rzut piętra 12 w budynku przy Al. Jerozolimskich 136.
4) Załącznik nr 4 – Rzut piętra 13 w budynku przy Al. Jerozolimskich 136.

Załącznik nr 1 - Wzór protokołu komisyjnego otwarcia pomieszczenia/szafy/sejfu

**ZATWIERDZAM** Dnia ……

**DYREKTOR GENERALNY GDOŚ**

…….

**PROTOKÓŁ**

**KOMISYJNEGO OTWARCIA POMIESZCZENIA/SZAF PODLEGAJĄCYCH ZABEZPIECZENIU/SEJFU**

W dniu ……r., komisja w składzie:

1) ……;

2) ……;

3) …….

powołana przez Dyrektora Generalnego GDOŚ w dniu …….. dokonała otwarcia pomieszczenia/pomieszczeń nr ……../szaf podlegających zabezpieczeniu/sejfu w pomieszczeniu nr...., zabezpieczonych w następujący sposób:

1) klucz – opis zabezpieczenia: …….

……..……

……..……..……

2) pomieszczenia, szafy podlegające zabezpieczeniu, znajdujące się w pomieszczeniu/ach – opis zabezpieczenia: ……..

……

……

Czynności dokonano w związku z nieobecnością prowadzącego sprawę i osoby go zastępującej, z uwagi na konieczność zapoznania się z następującymi dokumentami - wykonania następujących prac:

…….

…….

……

……..……..

Po dokonaniu tych czynności pomieszczenie nr ……../szafy podlegające zabezpieczeniu/sejf w pomieszczeniu nr ……., zabezpieczono w następujący sposób:

1) klucze – opis zabezpieczenia: ……..……

……..…….

…….

2) pomieszczenia, szafy podlegające zabezpieczeniu i biurka, znajdujące się w pomieszczeniu/ach – opis zabezpieczenia:

……..……..……

……..……..……

Pomieszczenie i worek/saszetkę z kluczami zabezpieczono przez plombowanie referentką/plombą nr .... będącą w dyspozycji członka komisji wskazanego w pkt ….. protokołu. Klucze zdeponowano do przechowania zgodnie z zasadami określonymi w § 5 ust. 2 zarządzenia.

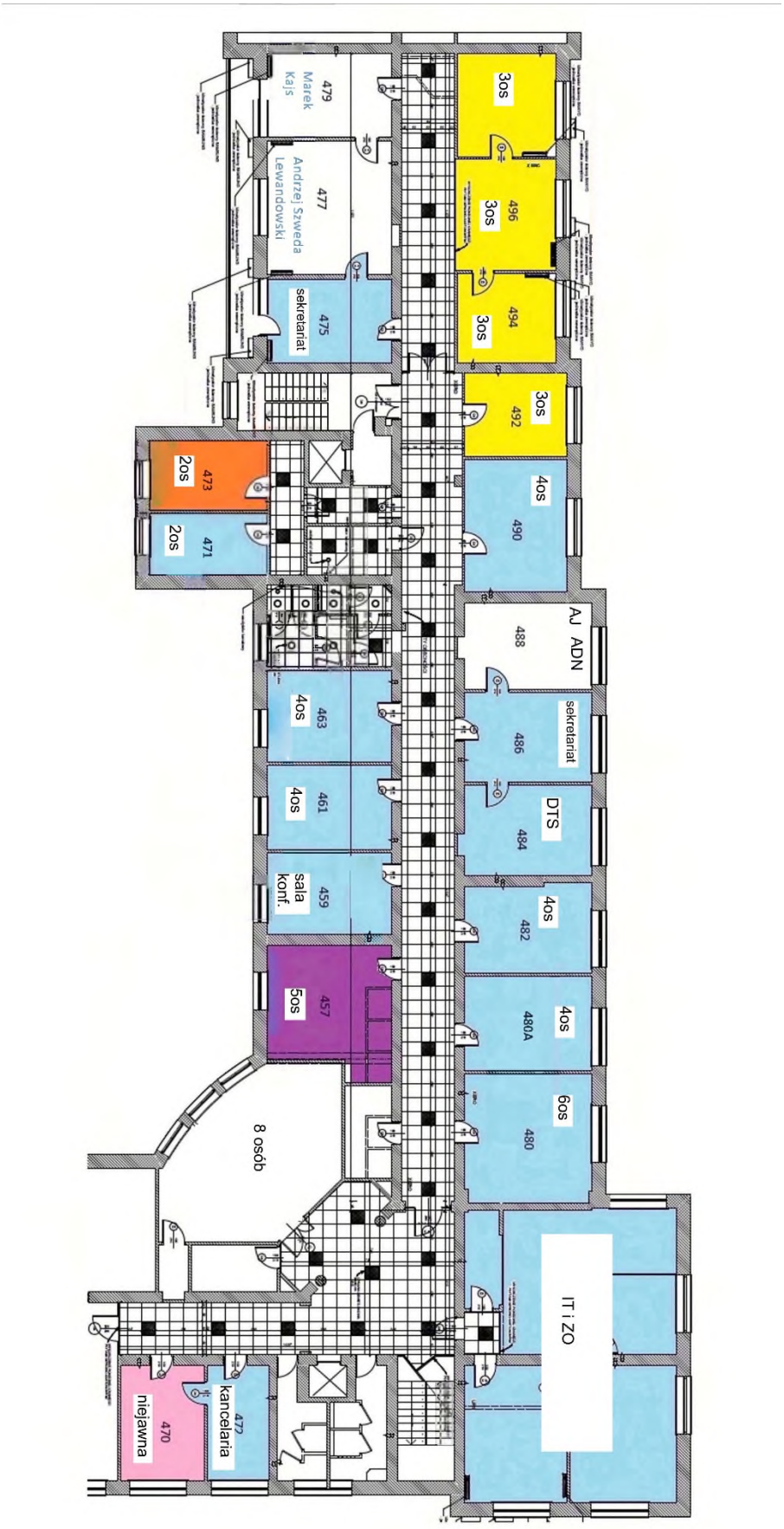
Podpisy członków komisji:

1) ……;

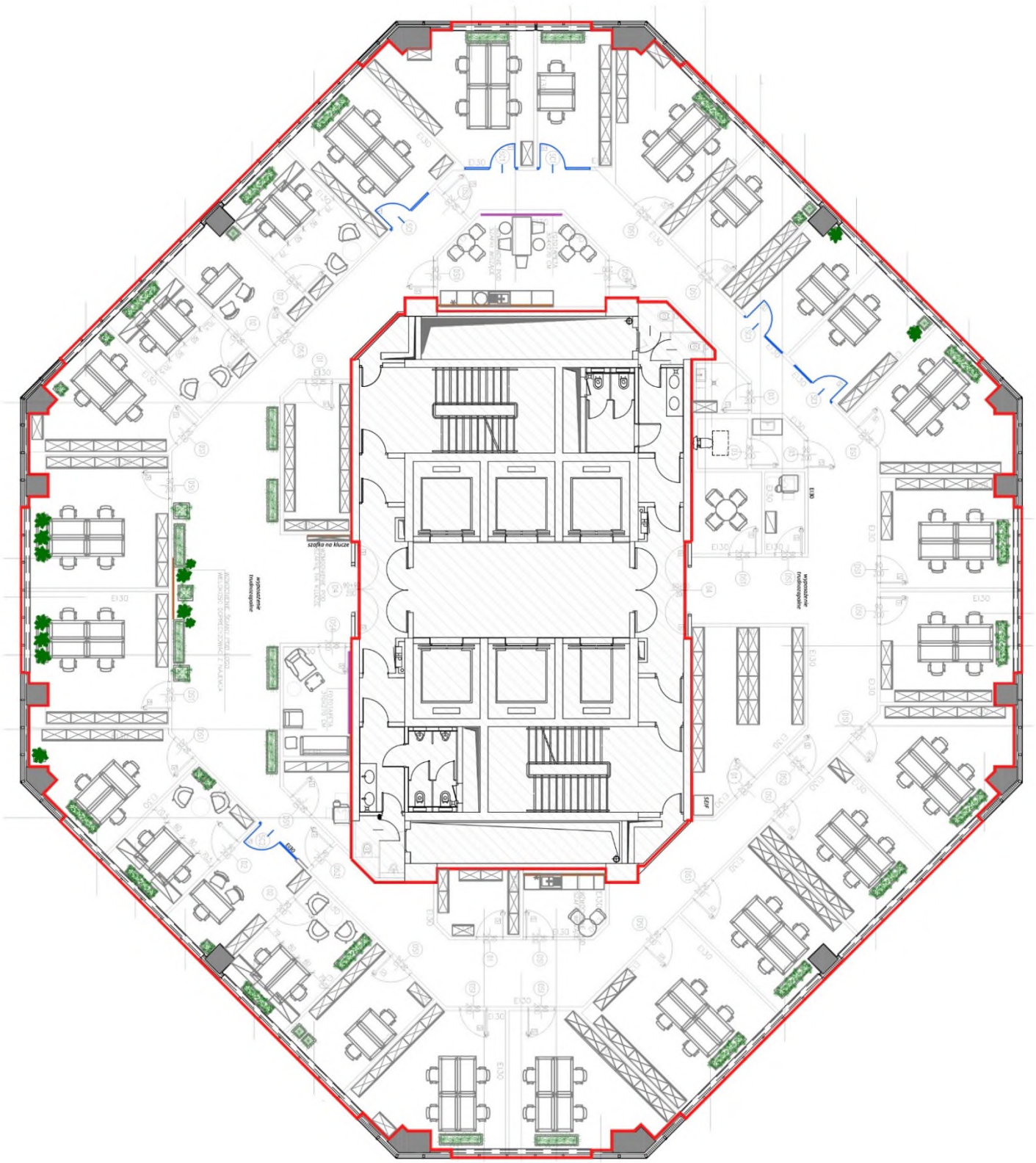
2) ……;

3) ……..

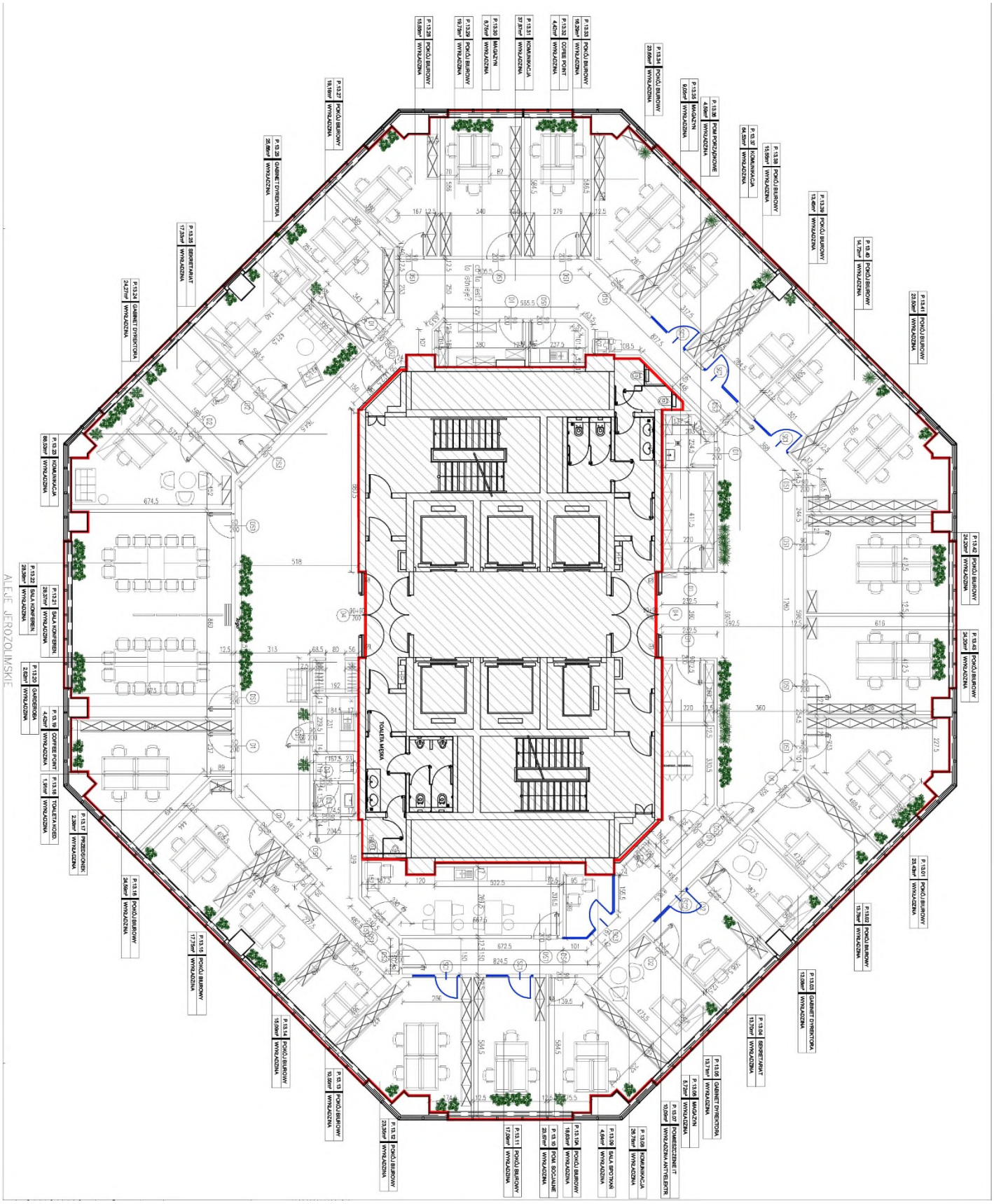
Załącznik nr 2 - rzut piętra IV w budynku przy ul Wawelskiej 52/56



Załącznik nr 3 - rzut piętra 12 w budynku przy Al. Jerozolimskich 136



Załącznik nr 4 - rzut piętra 13 w budynku przy Al. Jerozolimskich 136



**Załącznik nr 10** do Zarządzenia nr 6 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 15 listopada 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska

# *Zasady bezpieczeństwa w relacjach z Dostawcami w Generalnej Dyrekcji Ochrony Środowiska*

ZATWIERDZAM

Dyrektor Generalny

Generalnej Dyrekcji Ochrony Środowiska

Agnieszka Chilmon

Dyrektor Generalny

.....

Dyrektor Generalny

/ – podpisany cyfrowo/

| KARTA ZMIAN: | | | |
|---|---|---|---|
| Nr | Opis dokonanej zmiany w treści dokumentu | Data zmiany | Podpis uprawnionego pracownika |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

## Spis treści

## § 1. Cel

Celem niniejszego dokumentu jest przedstawienie ram w zakresie bezpieczeństwa informacji dla Dostawców, którzy mają dostęp w związku z zawartymi umowami do informacji chronionych Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ" oraz określenie minimalnych wymagań dotyczących zabezpieczeń systemów informatycznych Dostawców.

## § 2. Zakres

Postanowienia opisane w niniejszym dokumencie stosuje się do Dostawców, którzy zawarli umowę z GDOŚ.

## § 3. Terminologia

Ilekroć w niniejszych Zasadach jest mowa o:

1) **Dostawcy (Wykonawca, Podmiot Trzeci)** – należy przez to rozumieć podmiot świadczący lub dostarczający usługi lub produkty dla GDOŚ.
2) **Pełnomocniku ds. Bezpieczeństwa Informacji (Pełnomocnik ds. BI)** – należy przez to rozumieć osobę wyznaczoną przez Dyrektora Generalnego GDOŚ, która sprawuje nadzór nad wszystkimi czynnościami w obszarze zarządzania bezpieczeństwem informacji GDOŚ.
3) **Pracowniku** – należy przez to rozumieć osobę, która świadczy pracę na rzecz GDOŚ bez względu na podstawę (umowa o pracę, umowa cywilnoprawna, staż, praktyki, itp.).
4) **Przetwarzaniu danych** – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nie zautomatyzowany, takich jak zbieranie, przeglądanie, utrwalanie organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
5) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – należy przez to rozumieć system, na który składają się: polityki, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji dążącym do osiągnięcia celów GDOŚ.

## § 4. Odpowiedzialność i uprawnienia

1. Za nadzór nad stosowaniem niniejszych zasad odpowiada ze strony GDOŚ Pracownik odpowiedzialny za koordynację współpracy z Dostawcą oraz Dostawca, który został zobowiązany do jego przestrzegania w związku z zawartą z GDOŚ umową.
2. Zakres odpowiedzialności i uprawnień poszczególnych osób realizujących zadania w ramach niniejszych zasad został określony w **Polityce Bezpieczeństwa Informacji.**

## § 5. Zasady stosowania

1. W GDOŚ zasady współpracy z Dostawcami, w szczególności udzielanie dostępu (fizycznego i logicznego) do zasobów teleinformatycznych i Systemów teleinformatycznych GDOŚ są określone w zawieranych z Dostawcami umowach cywilnoprawnych zawierających postanowienia zobowiązujące do zachowania poufności i nieujawniania informacji. Umowy te precyzują wymagania bezpieczeństwa, jakie muszą spełniać Dostawcy, aby uzyskać dostęp do zasobów teleinformatycznych i Systemów teleinformatycznych GDOŚ.
2. Dostęp do informacji chronionych, w tym zasobów teleinformatycznych i Systemów teleinformatycznych GDOŚ nie może zostać przyznany Dostawcom, dopóki nie zostanie podpisana umowa o zachowaniu poufności. Każdy pracownik Dostawcy mający dostęp do informacji chronionych GDOŚ jest zobowiązany do podpisania ***Oświadczenia o stosowaniu zapisów Zasad bezpieczeństwa w relacjach z Dostawcami***, którego wzór stanowi załącznik nr 1 do niniejszego dokumentu. Jeżeli realizacja umowy związana jest z powierzeniem do Przetwarzania danych, Dostawca musi podpisać z GDOŚ stosowną umowę powierzenia Przetwarzania danych, jak również spełnić wymagania jakie stawia przed podmiotem przetwarzającym Rozporządzenie RODO.
3. Pracownik odpowiedzialny za przygotowanie umowy z Dostawcą, każdorazowo uwzględnia w jej treści zasady bezpieczeństwa informacji wynikające z SZBI w zakresie adekwatnym do przedmiotu umowy.
4. Zasady bezpieczeństwa w relacjach z Dostawcami GDOŚ obejmują swym zakresem wszystkie podmioty, będące Dostawcami produktów lub usług, mające dostęp do informacji chronionych GDOŚ.
5. GDOŚ powinien w regularnych odstępach czasu, tj. nie rzadziej niż co 12 miesięcy, dokonywać przeglądu usług świadczonych przez Dostawców. Za przeprowadzenie przeglądu odpowiada Pełnomocnik ds. BI, który sporządza raport z przeglądu usług świadczonych przez Dostawców, a następnie przedstawia go Dyrektorowi Generalnemu GDOŚ.
6. GDOŚ zarządza zmianami w zakresie świadczenia usług przez Dostawców. W razie konieczności GDOŚ aktualizuje dokumentację SZBI z uwzględnieniem krytyczności informacji, systemów i procesów, których dotyczą zmiany oraz ponownego szacowania ryzyka. Za aktualizację dokumentacji SZBI odpowiada Pełnomocnik ds. BI.
7. Zasady postępowania Dostawców dla dokumentów papierowych i danych elektronicznych zawierających informacje chronione GDOŚ muszą być zgodne z minimalnymi wymaganiami bezpieczeństwa informacji GDOŚ.

Załącznik nr 1 – Wzór oświadczenia pracownika Dostawcy o stosowaniu zapisów Zasad bezpieczeństwa w relacjach z Dostawcami

Warszawa, dnia ……

……
Imię i nazwisko pracownika Dostawcy

……
Nazwa (Dostawca)

## Oświadczenie

Oświadczam, że zapoznałam/zapoznałem się z treścią zapisów *Zasad bezpieczeństwa w relacjach z Dostawcami*, będących elementem Systemu Zarządzania Bezpieczeństwem Informacji Generalnej Dyrekcji Ochrony Środowiska i zobowiązuję się do ich przestrzegania.

Ponadto, zobowiązuję się do:

1. Zachowania w tajemnicy informacji chronionych, których właścicielem jest Generalna Dyrekcja Ochrony Środowiska, w szczególności sposobów ich zabezpieczenia, zarówno w trakcie jak i po zakończeniu wykonywania zadań objętych umową/wykonywanych w celu realizacji umowy nr […] zawartej dnia […].
2. Niewykorzystywania żadnych informacji chronionych Generalnej Dyrekcji Ochrony Środowiska w celu innym niż wykonywanie ww. zadań.

……

Podpis