DECYZJA nr 35/2023
Zarządu OPEC Sp. o.o. z siedzibą w Gdyni
z dnia 27.06.2023 r.

w sprawie: wprowadzenia Polityki Ochrony Danych Osobowych w OPEC Sp. z o.o.

Działając na podstawie § 14 ust. 1 i 2 Umowy Spółki oraz § 3 ust. 2 i ust. 6 Regulaminu Zarządu OPEC Sp. z o.o. zgodnie z art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO) (Dz. Urz. UE L 119, s. 1), ustanawia się, co następuje:

§ 1

1. Wprowadza się Politykę Ochrony Danych Osobowych (wersja 6.0) w OPEC Sp. z o.o. [zwana dalej: Polityką], stanowiącą załącznik do niniejszej Decyzji.
2. Politykę stosuje się do przetwarzania danych osobowych przez upoważnionych pracowników OPEC.
3. Za bezpieczeństwo przetwarzania danych osobowych w systemach elektronicznych odpowiedzialny jest Administrator Systemów Informatycznych (ASI).

§ 2

Zobowiązuje się:

1. kierowników i koordynatorów komórek organizacyjnych OPEC do zapoznania podległych im pracowników z treścią Polityki, o której mowa w § 1, szczególnie z zasadami przetwarzania danych, a także do nadzoru nad jej przestrzeganiem;
2. Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych do zapoznania nowo zatrudnianych pracowników z niniejszą Polityką;
3. wszystkich pracowników do zapoznania się i stosowania zasad, procedur i instrukcji określonych w Polityce i załącznikach do niej.

§ 3

1. Procedury, instrukcje oraz inne schematy postępowania regulujące poszczególne obszary dotyczące realizacji zasad i obowiązków wynikających z Polityki oraz RODO posiadają status obowiązujący po zatwierdzeniu przez Inspektora Ochrony Danych i Administratora Systemów Informatycznych (w ramach swoich kompetencji).
2. Inspektor Ochrony Danych o wdrożeniu nowych regulacji dotyczących ochrony danych osobowych, o których mowa w ust. 1 powyżej lub aktualizacji istniejących procedur, informuje kierowników i koordynatorów komórek OPEC drogą elektroniczną, a obowiązujące wersje dokumentów zamieszcza w repozytorium dokumentów OPEC.

§ 4

1. Uchyla się Politykę Ochrony Danych Osobowych w OPEC Sp. z o.o. zatwierdzoną dnia 1.02.2021 r.
2. Decyzja wchodzi w życie z dniem podjęcia.

PREZES ZARZĄDU
OPEC Sp. z o.o.
Wojciech Polejewski

Załącznik:
1. Polityka Ochrony Danych Osobowych (wersja 6.0) w OPEC Sp. z o.o.

Rozdzielnik:
1. Wszystkie komórki organizacyjne
2. Biuro Zarządu a/a

Okręgowe Przedsiębiorstwo Energetyki Cieplnej sp. z o.o.
Polityka ochrony danych osobowych

Okręgowe Przedsiębiorstwo Energetyki Cieplnej
Spółka z ograniczoną odpowiedzialnością
81-213 Gdynia, ul. Opata Hackiego 14

ZATWIERDZAM
Prezes Zarządu

PREZES ZARZĄDU
OPEC Sp. z o.o.
Wojciech Polejewski
(data i podpis)

POLITYKA OCHRONY DANYCH OSOBOWYCH

DOKUMENTACJA OPISUJĄCA SPOSÓB PRZETWARZANIA

DANYCH OSOBOWYCH ORAZ ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE ICH OCHRONĘ

(wersja 6.0)

Gdynia - 2023 r.

INSPEKTOR OCHRONY DANYCH
Okręgowego Przedsiębiorstwa Energetyki Cieplnej
Spółka z o.o. w Gdyni
mgr Tomasz Hopcia

KIEROWNIK
Działu IT
Dariusz Witt

RADCA PRAWNY
Paweł Zamiński

1

Polityka Ochrony Danych Osobowych
W Okręgowym Przedsiębiorstwie Energetyki Cieplnej Spółka z o.o. w Gdyni

Spis treści

Rozdział I

Postanowienia wstępne
§ 1

1. Polityka ochrony danych osobowych w Okręgowym Przedsiębiorstwie Energetyki Cieplnej Spółka z o.o. w Gdyni jest zbiorem zasad i procedur, obowiązujących przy realizacji wszystkich czynności przetwarzania danych osobowych przez OPEC i Prezesa Zarządu..
   Celem wprowadzania Polityki jest ograniczenie ryzyka naruszenia praw i wolności osób fizycznych, w tym w szczególności , klientów OPEC i pracowników jednostki, jakie może spowodować przetwarzania ich danych w związku z realizowanymi przez OPEC i Prezesa Zarządu OPEC zadaniami i obowiązkami. Ponadto Polityka ma na celu wykazanie realizacji zasady rozliczalności, przez prowadzenie w OPEC odpowiedniej dokumentacji, opisującej sposoby ochrony danych, na którą składa się niniejsza Polityka wraz z załącznikami stanowiącymi jej integralną część.
2. Niniejsza Polityka ochrony danych osobowych została opracowana i wdrożona w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie aktów prawnych, w szczególności:
   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),
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
   3) Ustawy z dnia 21 lutego 2019r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 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.U. z 2019r. poz. 730).
   4) Wskazówek Prezesa UODO dotyczące wykorzystania monitoringu wizyjnego.

   oraz w celu zapewnienia integralności z wdrożonym w OPEC systemem zarządzania bezpieczeństwem informacji.

3. Polityka ochrony danych osobowych ma zastosowanie we wszystkich komórkach organizacyjnych Okręgowego Przedsiębiorstwa Energetyki Cieplnej Spółka z o.o. w Gdyni.
4. Dane osobowe w Okręgowym Przedsiębiorstwie Energetyki Cieplnej Spółka z o.o. w Gdyni mogą być przetwarzane zarówno w sposób tradycyjny w księgach, aktach, wykazach i innych papierowych zbiorach ewidencji, jak i w systemach informatycznych.
5. Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Prezes Zarządu Okręgowego Przedsiębiorstwa Energetyki Cieplnej Spółka z o.o. w Gdyni.

Słownik terminów
§ 2

1. Definicje, skróty oraz konwencje zwrotów stosowanych w niniejszej Polityce:
   dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, w szczególności takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden bądź więcej szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną

tożsamość tej osoby fizycznej;
przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych i obejmuje w szczególności zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wyszukiwanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie danych osobowych;
Administrator (Danych Osobowych - ADO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych tj. Administratorem Danych Osobowych, w rozumieniu art. 4 pkt 7 RODO, jest Okręgowe Przedsiębiorstwo Energetyki Cieplnej Spółka z o.o. w Gdyni ponieważ administratora danych osobowych (ADO) reprezentuje Zarząd (zgodnie bowiem z k.s.h. zarząd posiada prawo reprezentowania administratora danych osobowych oraz prowadzi sprawy spółki).reprezentantem ADO w OPEC Spółka z o.o. w Gdyni jest Prezes Zarządu.
Administrator Systemów Informatycznych (ASI) – osoba lub podmiot wyznaczony przez administratora danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez administratora danych;
Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Prezesa Zarządu Okręgowego Przedsiębiorstwa Energetyki Cieplnej Spółka z o.o. w Gdyni koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w i OPEC pod kątem zgodności z przepisami;
organ nadzorczy - Prezes Urzędu Ochrony Danych (PUOD) – niezależny krajowy organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych oraz ułatwienia swobodnego przepływu danych osobowych w Unii;
naruszenie ochrony danych osobowych – 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;
podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych;
państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego;
Polityka ODO – Polityka ochrony danych osobowych w Okręgowym Przedsiębiorstwie Energetyki Cieplnej Spółka z o.o. w Gdyni;
RCPD – Rejestr czynności przetwarzania danych;
RKCP – Rejestr kategorii czynności przetwarzania;
RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
OPEC – Okręgowe Przedsiębiorstwo Energetyki Cieplnej Spółka z o.o. w Gdyni;
Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
Komórka Organizacyjna - należy przez to rozumieć wyodrębnione w strukturze jednostki zakłady, działy, zespoły lub samodzielne stanowiska;
Kierownik komórki organizacyjnej – należy przez to rozumieć kierowników zakładów, działów oraz koordynatorów zespołów
Osoba upoważniona do przetwarzania danych osobowych lub użytkownik systemu – osoba, która została upoważniona pisemnie przez ADO oraz dopuszczona,

jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu;
Pracownik – osoba współpracująca z administratorem danych na podstawie umowy o pracę lub umowy cywilnoprawnej.

Rozdział II
Organizacja i zasady przetwarzania danych osobowych

§ 3

1. Przetwarzanie danych osobowych w OPEC jest dopuszczalne wyłącznie pod warunkiem przestrzegania przepisów RODO, ustawy oraz polityk, procedur i instrukcji wewnętrznych wdrożonych w Okręgowym Przedsiębiorstwie Energetyki Cieplnej Spółka z o.o. w Gdyni.
2. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z w/w regulacjami odpowiada:
   1) Administrator Danych Osobowych (ADO),
   2) Inspektor Ochrony Danych Osobowych (IOD),
   3) Administrator systemów informatycznych (ASI),
   4) Osoby upoważnione do przetwarzania danych osobowych.
3. Administratorem danych osobowych w rozumieniu art. 4 pkt 7 RODO, jest Okręgowe Przedsiębiorstwo Energetyki Cieplnej Spółka z o.o. w Gdyni ponieważ administratora danych osobowych (ADO) reprezentuje Zarząd (zgodnie bowiem z k.s.h. zarząd posiada prawo reprezentowania administratora danych osobowych oraz prowadzi sprawy spółki) reprezentantem ADO w OPEC Spółka z o.o. w Gdyni jest Prezes Zarządu, który przetwarza dane osobowe klientów oraz pracowników OPEC .

§ 4

1. OPEC przetwarza dane osobowe zgodnie z zasadami wskazanymi w art. 5 i art. 25 RODO, które stanowią filary ochrony danych osobowych, tj. zgodnie z zasadą:
   1) zgodności z prawem,
   2) rzetelności i przejrzystości,
   3) zasadą ograniczenia celu,
   4) minimalizacji danych,
   5) prawidłowości danych,
   6) ograniczenia przechowywania,
   7) integralności i poufności,
   8) ochrony danych w fazie projektowania,
   9) domyślną ochroną danych,
   10) zasadą przestrzegania praw podmiotu danych osobowych.
2. Zasada zgodności z prawem (art. 5 ust. 1 lit. a RODO) oznacza, że OPEC przetwarza dane osobowe na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych wynikających z art. 6, 9 RODO.OPEC jako spółka z o.o., realizuje zadania wynikające z przedmiotu działalności Spółki zgodnie z Polską Klasyfikacją Działalności i co do zasady przetwarzanie danych osobowych w jednostce odbywa się w oparciu o przesłanki wskazane w art. 6 ust. 1 lit. b, lub art. 9 ust. 2 lit.. Stosowanie przedmiotowej zasady oznacza zobowiązanie pracowników OPEC – w odniesieniu do realizowanych czynności przetwarzania danych osobowych – do identyfikowania podstawy prawnej w postaci konkretnej normy prawnej i jej wskazanie w Rejestrze czynności przetwarzania danych osobowych (RCPD). Wzór rejestru stanowi **załącznik nr 1 do Polityki ODO i w wersji do edycji jest dostępny w repozytorium OPEC folder Polityka Ochrony Danych Osobowych**.
3. W uzasadnionych przypadkach przetwarzanie danych osobowych przez OPEC może odbywać się z art. 6 ust.1 lit. a RODO tj. jeśli podstawę przetwarzania stanowi zgoda osoby, której dane dotyczą na przetwarzanie danych w zakresie i celu określonym w treści zgody lub przesłankę z art. 6 ust.1 lit. b RODO tj. jeśli przetwarzanie danych jest niezbędne do wykonania umowy lub podjęcia działań przed zawarciem umowy.

4. Przetwarzanie danych osobowych w oparciu o przesłankę z art. 6 ust. 1 lit. d RODO dotyczy sytuacji szczególnych tj. jeśli przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej.
5. Rejestr czynności przetwarzania danych osobowych jest prowadzony dla OPEC z rozbiciem na poziomie każdej komórki organizacyjnej, w tym również na samodzielnych stanowiskach pracy. Za prowadzenie przedmiotowego rejestru, odpowiedzialny jest Inspektor Ochrony Danych Osobowych .
6. Zasadę rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO) OPEC realizuje poprzez wypełnianie obowiązków informacyjnych wskazanych w art. 13 i art. 14 RODO oraz udzielanie odpowiedzi na wnioski osób, których dotyczą, szczególnie w zakresie wynikającym z art. 15 RODO. Obowiązki informacyjne realizowane są przez poszczególnych pracowników OPEC, którym powierzono prowadzenie sprawy lub jej prowadzenie wynika z przyjętego zakresu obowiązków. Za prawidłową realizację przedmiotowego obowiązku informacyjnego odpowiada pracownik oraz jego bezpośredni przełożony.
7. Prezes Zarządu OPEC jako administrator przetwarza dane osobowe głównie w celach związanych z realizacją zadań zawartych w przedmiocie działalności Spółki .Wyjątek stanowi dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (zasady dotyczące przetwarzania danych osobowych art. 5 ust. 1 lit. b RODO). Wskazanie celu przetwarzania stanowi obowiązkowy element Rejestru czynności przetwarzania danych osobowych oraz informacji udzielanej właścicielowi danych osobowych.
8. OPEC , jako podmiot przetwarzający w sytuacji, gdy na mocy pisemnej umowy lub innego instrumentu prawnego powierzono jemu dane innego administratora, będzie przetwarzał powierzone dane w imieniu i na rzecz administratora (art. 30 ust. 2 RODO), zobowiązany jest prowadzić Rejestr kategorii czynności przetwarzania (RKCP). Wzór RKCP stanowi **załącznik nr 2 do Polityki ODO i w wersji do edycji dostępny jest w repozytorium OPEC folder Polityka Ochrony Danych Osobowych.**
9. Rejestr kategorii czynności przetwarzania oraz Rejestr czynności przetwarzania danych osobowych stanowią formę dokumentowania czynności przetwarzania danych osobowych i są kluczowymi elementami umożliwiającymi realizację zasady rozliczalności.
10. Dla celów zgodności z zasadą minimalizacji danych (art. 5 ust. 1 lit.c RODO) w OPEC przetwarza się wyłącznie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania, a osoba przetwarzająca w kontekście realizowanego zadania jest w stanie uzasadnić potrzebę przetwarzania każdej kategorii i każdego rodzaju danych. Za adekwatność zakresu przetwarzanych danych osobowych ponosi odpowiedzialność pracownik realizujący czynność przetwarzania i jego bezpośredni przełożony. Kategorie danych podlegające przetwarzaniu muszą znaleźć swoje odzwierciedlenie w Rejestrze czynności przetwarzania danych osobowych, o których mowa w art. 30 ust. 1 RODO, w odniesieniu do konkretnie realizowanej czynności przetwarzania .
11. Przetwarzaniu podlegają dane osobowe prawidłowe, aktualne i odpowiadające faktycznemu stanowi rzeczy, co spełnia wymagania zasady prawidłowości danych (art.5 ust. 1 lit. d RODO). Do obowiązków pracownika przetwarzającego dane jest podjęcie starań w celu upewnienia się co do stanu aktualności przetwarzanych danych osobowych.
12. Dane osobowe w OPEC przetwarza się wyłącznie przez okres niezbędności dysponowania dokumentacją dla zrealizowania celu załatwienia sprawy, a następnie archiwizuje przez okres wynikający z Jednolitego rzeczowego wykazu akt, odpowiadający wymogom ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
13. W OPEC proces przetwarzania danych osobowych odpowiada zasadzie integralności i poufności (art. 5 ust. 1 lit. f RODO). Dopuszcza się do przetwarzania danych osobowych jedynie osoby odpowiednio upoważnione i stosuje się odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
14. Przetwarzanie danych osobowych - w zakresie działania OPEC - w systemie

informatycznym lub/i papierowej odbywa się na polecenie ADO osobom, które potwierdziły zapoznanie się z obowiązującymi przepisami w tym zakresie.

15. OPEC wdrożył zasady dostępu do danych (w tym osobowych) i systemach informatycznych oraz zasady zarządzania uprawnieniami użytkowników w Polityce Ochrony Danych Osobowych, która dostępna jest w **repozytorium/ RODO załącznik nr 4 do Polityki Ochrony Danych Osobowych.**

16. Celem aktualizacji zapisów w Rejestrze czynności przetwarzania danych osobowych i w Rejestrze kategorii czynności przetwarzania administrator danych osobowych przeprowadza okresową inwentaryzację, która wykonywana jest co najmniej raz do roku przez Inspektora Ochrony Danych.

Rozdział III
Obowiązek informacyjny i obsługa praw

§ 5

1. OPEC wypełnia obowiązki informacyjne w stosunku do osób, których dane przetwarza oraz zapewnia obsługę ich praw realizując otrzymane żądania w szczególności:
   a) przekazuje informacje właścicielom danych osobowych lub ich opiekunom prawnym w formie informacji zgodnie z zapisami art. 13 oraz art. 14 RODO;
   b) weryfikuje i zapewnia możliwość wykonania żądania w ramach przyjętej struktury organizacyjnej OPEC;
   c) zapewnia odpowiednie środki organizacyjne i techniczne, aby żądania zrealizowano w terminach określonych w RODO. Bezpośredni nadzór nad realizacją zgłaszany żądań sprawuje administrator danych osobowych.
2. OPEC dba o jasną i czytelną formę przekazywanych informacji i komunikacji, których dane przetwarza.
3. OPEC poprzez m.in. zamieszczenie na swojej stronie internetowej, w BIP, poczcie elektronicznej, klauzulach informacyjnych oraz odwołań do informacji o prawach osób i sposobie korzystania z nich również w postaci linków ułatwia osobom korzystanie z ich praw.
4. OPEC informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych – chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.
5. W przypadku stwierdzonego naruszenia ochrony danych osobowych, OPEC bez zbędnej zwłoki zawiadomi właściciela danych, jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw i wolności tej osoby (art. 34 RODO).

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w OPEC stanowi **załącznik nr 8 do Polityki Ochrony Danych Osobowych .**

Rozdział IV
Administrator Danych Osobowych (ADO)

§ 6

1. Administratorem Danych Osobowych w rozumieniu art. 4 pkt 7 RODO jest Okręgowe Przedsiębiorstwo Energetyki Cieplnej Spółka z o.o. w Gdyni ponieważ administratora danych osobowych (ADO) reprezentuje zarząd (zgodnie bowiem z k.s.h. zarząd posiada prawo reprezentowania administratora danych osobowych oraz prowadzi sprawy spółki)reprezentantem ADO w OPEC Spółka z o.o. w Gdyni jest Prezes Zarządu.
2. Głównym zadaniem ADO jest ustalenie charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw i wolności osób fizycznych i wdrożenie odpowiednich środków technicznych i organizacyjnych, mających na celu zapewnienie procesowi przetwarzania zgodności z przepisami wskazanymi w RODO.

3. Obowiązki ADO określone w przepisach o ochronie danych osobowych :

Opis obowiązku ADO	Podstawa prawna	Sankcja karna
Przestrzeganie zasad dotyczących przetwarzania danych osobowych: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność, rozliczalność.	art. 5 RODO	art. 83 ust. 5 pkt a RODO
Spełnianie warunków zgodności z prawem przetwarzania danych - dobór właściwych przesłanek legalizujących przetwarzanie.	art. 6 RODO	art. 83 ust. 5 pkt a RODO
Dochowanie warunków wyrażenia zgody przez osobę, której dane dotyczą, na przetwarzanie danych osobowych.	art. 7 RODO	art. 83 ust. 5 pkt a RODO
Dochowanie warunków wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego.	art. 8 RODO	art. 83 ust. 4 pkt a RODO
Respektowanie zakazu przetwarzania danych osobowych **szczególnej kategorii**, jeżeli ADO nie może powołać się na przesłanki określone w art. 9 ust. 2 RODO.	art. 9 ust. 1 i 2 RODO	art. 83 ust. 5 pkt a RODO
W przypadku posiadania przez ADO statusu współadministratora przestrzeganie uzgodnionych zakresów swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.	art. 26 ust. 1 RODO	art. 83 ust. 4 pkt a RODO
Udostępnianie podmiotom, których dane dotyczą informacji o zasadniczej treści uzgodnień zawartych przez współadministratorów.	art. 26 ust. 2 RODO	art. 83 ust. 4 pkt a RODO
Zapewnienie przejrzystego informowania i przejrzystej komunikacji oraz trybu wykonywania praw przez osobę, której dane dotyczą.	art. 12 RODO	art. 83 ust. 5 pkt b RODO
Wykonywanie podczas pozyskiwania danych obowiązków informacyjnych wobec osoby, której dane dotyczą.	art. 13 RODO	art. 83 ust. 5 pkt b RODO
Wykonywanie obowiązków informacyjnych wobec osoby, której dane dotyczą, w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą.	art. 14 RODO	art. 83 ust. 5 pkt b RODO
Zapewnienie prawa dostępu do informacji o przetwarzaniu jej danych osobie, której dane dotyczą.	art. 15 RODO	art. 83 ust. 5 pkt b RODO

Opis obowiązku ADO	Podstawa prawna	Sankcja karna
Respektowanie prawa osoby, której dane dotyczą do: • sprostowania danych • usunięcia danych („prawo do bycia zapomnianym") • ograniczenia przetwarzania • przenoszenia danych • sprzeciwu.	art. 16 RODO art. 17 RODO art. 18 RODO art. 20 RODO art. 21 RODO	art. 83 ust. 5 pkt b RODO
Informowanie o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których ADO dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcy, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.	art. 19 RODO	art. 83 ust. 5 pkt b RODO
Prowadzenie z osobą, której dane dotyczą komunikacji w sprawie przetwarzania, w tym udzielnie osobie, której dane dotyczą, informacji o działaniach podjętych w związku z określonym żądaniem.	art. 15–22 i 34 RODO	art. 83 ust. 5 pkt b RODO
Przestrzeganie wymogów odnoszących się do zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania.	art. 22 RODO	art. 83 ust. 5 pkt b RODO
Wdrażanie odpowiednich środków technicznych i organizacyjnych zapewniających przetwarzanie danych zgodnie z RODO, w tym odpowiednich polityk ochrony danych oraz - dobrowolnie: zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji.	art. 24 RODO	art. 83 ust. 4 pkt a RODO
Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych (pseudonimizacja, minimalizacja danych).	art. 25 RODO	art. 83 ust. 4 pkt a RODO
Wdrażanie odpowiednich środków technicznych i organizacyjnych zapewniających właściwy stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych (pseudonimizacja i szyfrowanie danych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania).	art. 32 RODO	art. 83 ust. 4 pkt a RODO
Prowadzenie rejestru czynności przetwarzania danych osobowych, z uwzględnieniem zastrzeżenia, o którym mowa w art. 30 ust. 5 RODO.	art. 30 ust. 1 RODO	art. 83 ust. 4 pkt a RODO

Opis obowiązku ADO	Podstawa prawna	Sankcja karna
Nadawanie i wycofywanie upoważnień do przetwarzania danych osobowych.	art. 32 ust. 4 RODO	art. 83 ust. 4 pkt a RODO
Przestrzeganie zasady szczególnej staranności przy doborze podmiotu przetwarzającego dane w imieniu ADO. .	art. 28 ust. 1 RODO	art. 83 ust. 4 pkt a RODO
Powierzenie przetwarzania danych na podstawie umowy lub innego instrumentu prawnego, które wiążą podmiot przetwarzający i ADO.	art. 28 ust. 3 RODO	art. 83 ust. 4 pkt a RODO
Wyrażanie zgody lub nieaprobowanie podpowierzenia przetwarzania danych przez podmiot przetwarzający.	art. 28 ust. 2 i 4 RODO	art. 83 ust. 4 pkt a RODO
Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.	art. 33 ust. 1 i 3 RODO	art. 83 ust. 4 pkt a RODO
Dokumentowanie wszelkich naruszeń ochrony danych, w tym okoliczności naruszeń, ich skutków oraz podjętych działań zaradczych.	art. 33 ust. 5 RODO	art. 83 ust. 4 pkt a RODO
Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.	art. 34 RODO	art. 83 ust. 4 pkt a RODO
Wyznaczenie inspektora ochrony danych, jeśli nie zachodzą przesłanki zwalniające ADO.	art. 37 RODO	art. 83 ust. 4 pkt a RODO
Opublikowanie danych kontaktowych inspektora ochrony danych i zawiadomienie o nich organu nadzorczego.	art. 37 ust. 7 RODO	art. 83 ust. 4 pkt a RODO
Zapewnienie inspektorowi ochrony danych wymaganego w RODO statusu oraz zasobów niezbędnych do wykonania zadań inspektora oraz dostępu do danych osobowych i operacji przetwarzania, a także zasobów niezbędnych do utrzymania jego wiedzy fachowej.	art. 37 ust. 2 RODO	art. 83 ust. 4 pkt a RODO
Dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych (DPIA), jeśli ADO nie jest zwolniony z tego obowiązku.	art. 35 RODO	art. 83 ust. 4 pkt a RODO
Przestrzeganie przepisów dotyczących przekazywania danych osobowych do państw trzecich.	rozdział V RODO	art. 83 ust. 5 pkt c RODO
Przestrzeganie zasad odstępstwa lub wyjątków od określonych przepisów RODO dla przetwarzania danych do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej.	art. 85 RODO	
Przestrzeganie nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.	art. 58 ust. 1 i 2 RODO	art. 83 ust. 5 pkt e RODO

4. Aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać ADO odpowiada w szczególności za:
   a) wprowadzenie polityki ochrony danych osobowych;
   b) podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie;
   c) przejrzyste, terminowe i właściwe informowanie osób, których dane przetwarza o wszystkich okolicznościach przetwarzania oraz o przysługującym im prawach;
   d) organizowanie administrowania danymi oraz określenie właściwych sposobów zabezpieczania danych osobowych;
   e) upoważnianie poszczególnych osób adekwatnie do zajmowanego stanowiska do czynności przetwarzania danych osobowych w zakresie odpowiadającym powierzonym czynnościom na danym stanowisku pracy (art. 29 RODO). Przy wydawaniu upoważnień administrator kieruje się zasadą wiedzy koniecznej w stosunku do osoby upoważnianej oraz prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych;
   f) odwołanie/anulowanie wcześniej wydanych upoważnień do przetwarzania danych osobowych;
   g) upoważnianie osób do przetwarzania danych osobowych poza obszarem administrowanym;
   h) upoważnianie osób do przetwarzania danych osobowych w systemach monitoringu wizyjnego
   i) wyznaczenie i powołanie Inspektora Ochrony Danych zgodnie z art. 37 i art. 38 RODO oraz wskazanie osoby lub podmiotu, który będzie administrował użytkowanymi w OPEC systemami informatycznymi (ASI) wraz z określeniem zakresu zadań tej osoby/podmiotu;
   j) podejmowanie w porozumieniu z IOD odpowiednich działań w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia przetwarzania danych osobowych, w tym w szczególności w przypadku konieczności jego niezwłocznego zgłoszenia organowi nadzorczemu (PUODO) - bez zbędnej zwłoki – nie później niż w terminie 72 godzin (art. 33 RODO);
   k) dokonywanie oceny ryzyka naruszenia praw lub wolności osób fizycznych, a gdy ryzyko to jest wysokie, oceny skutków przetwarzania dla ochrony danych osobowych (art. 35 RODO) w konsultacji z IOD;.
   l) zapewnienie pracownikom odpowiedniego wyposażenia stanowisk pracy i warunków pracy, umożliwiających przetwarzanie danych osobowych zgodnie z niniejszą Polityką;
   m) sprawowanie nadzoru nad przestrzeganiem przyjętych zasad ochrony danych osobowych;
   n) sprawowanie nadzoru nad działaniami osoby administrującej systemami informatycznymi w Spółce;
   o) dobór podmiotów przetwarzających dane na rzecz OPEC. Administrator określa wymagania w zakresie warunków przetwarzania w stosunku do podmiotów przetwarzających, zawiera z nimi stosowne umowy powierzenia danych osobowych oraz prowadzi rejestr umów powierzenia.

Rozdział V
Administrator systemów informatycznych (ASI)

§ 7

1. Funkcję Administratora systemów informatycznych pełni osoba lub podmiot wyznaczony przez Administratora danych.
2. ASI realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemami informatycznymi, w szczególności:
   a) nadzoruje i zarządza systemami informatycznymi, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
   b) konfiguruje wszystkie stacje robocze w jednostce w sposób zapewniający, że tylko

z pozycji administratora dostępne będą opcje związane z konfiguracją zainstalowanego systemu operacyjnego oraz instalacją i aktualizacją zainstalowanego oprogramowania;
c) opiniuje wszelkie przedsięwzięcia związane z wprowadzeniem nowych rozwiązań funkcjonalnych, oprogramowania oraz urządzeń w odniesieniu do funkcjonującego w OPEC systemu informatycznego. Wydane przez ASI opinie mogą mieć charakter wiążący i rozstrzygający;
d) sprawuje nadzór nad wdrożonymi oraz wdrażaniem nowych środków technicznych i organizacyjnych zapewniających ochronę systemów informatycznych;
e) opracowuje oraz aktualizuje ogólny opis techniczny środków bezpieczeństwa wdrożonych w Polityce Bezpieczeństwa Informacji OPEC w Gdyni ;
f) sprawuje nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
g) podejmuje wszelkie niezbędne działania w przypadku wykrycia naruszeń w systemie zabezpieczeń oraz rejestruje i analizuje informacje związane ze zgłaszanymi zdarzeniami w obszarze bezpieczeństwa IT;
h) identyfikuje i analizuje zagrożenia oraz ocenia ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
i) inicjuje i nadzoruje wdrażanie nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;
j) dokonuje cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych;
k) współpracuje z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych;
l) na wniosek kierownika komórki organizacyjnej określa dla użytkownika dostęp do poszczególnych zasobów informatycznych OPEC przydzielając każdemu z nich indywidualny login oraz dokonuje ewentualnych modyfikacji uprawnień dostępu do systemów informatycznych. W tym samym trybie wyrejestrowuje użytkowników systemu,
m) nadzoruje zasady przetwarzana danych osobowych w systemach monitoringu wizyjnego OPEC w Gdyni stanowiące **załącznik 10 do Polityki Ochrony Danych Osobowych,**
n) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń i nośników komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych i ich przechowywaniem oraz okresowym ich sprawdzaniem pod kątem dalszej przydatności do odtwarzania danych, w przypadku awarii systemu informatycznego;
o) określa wymagania w zakresie warunków powierzenia przetwarzania danych osobowych podmiotom świadczącym usługi informatyczne, zawiera z nimi stosowne umowy powierzenia oraz prowadzi rejestr tych umów;

§ 8

1. Administrator systemu informatycznego ma prawo do:
   a) wyznaczania, rekomendowania i egzekwowania wykonania zaleceń związanych z ochroną systemów informatycznych funkcjonujących w OPEC;
   b) opiniowania możliwości wdrażania i rozbudowy systemów informatycznych o dodatkowe elementy;
   c) wstępu do pomieszczeń w których użytkowane są systemy informatyczne i przeprowadzania niezbędnych badań lub innych czynności mających na celu zapewnienie prawidłowego funkcjonowania użytkowanych systemów informatycznych, w tym również poza godzinami pracy OPEC po wcześniejszym ustaleniu tego z ADO;
   d) wnioskowania o złożenie pisemnych lub ustnych wyjaśnień przez pracowników OPEC lub osób współpracujących w zakresie niezbędnym do ustalenia stanu faktycznego odnoszącego się do funkcjonowania systemów informatycznych oraz przyjętych zabezpieczeń;

e) wglądu do dokumentów, systemów i wszelkich danych mających bezpośredni związek z problematyką kontroli przyczyn naruszenia;
f) dokonywania oględzin urządzeń i nośników służących do przetwarzania danych w systemach informatycznych OPEC.

Rozdział VI
Inspektor Ochrony Danych (IOD)

§ 9

1. Prezes w Gdyni Okręgowego Przedsiębiorstwa Energetyki Cieplnej Spółka z o.o. w Gdyni. jako administrator obowiązany jest do wyznaczenia Inspektora Ochrony Danych zgodnie z zapisami art. 37 RODO.
2. Administrator danych osobowych zapewnia:
   a) włączenie IOD we wszystkie sprawy dotyczące ochrony danych ;
   b) wsparcie IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO;
   c) powstrzymanie się przed wydawaniem IOD instrukcji dotyczących sposobu wykonywania zadań przez IOD;

§ 10

1. Do zadań IOD należy:
   a) informowanie ADO oraz pracowników OPEC przetwarzających dane osobowe o obowiązkach spoczywających na nich na mocy niniejszej Polityki oraz innych przepisów, w tym w szczególności RODO i doradzanie im w zakresie ochrony danych osobowych;
   b) monitorowanie przestrzegania niniejszej Polityki, przepisów RODO, innych przepisów prawa związanych z ochroną danych, w tym podejmowanie działań zwiększających świadomość, szkolenie osób uczestniczących w operacjach przetwarzania oraz przeprowadzanie powiązanych z tym audytów;
   c) udzielanie – na wniosek administratora – zaleceń co do oceny skutków dla ochrony danych oraz monitorowania ich wykonania, zgodnie z art. 35 RODO;
   d) weryfikacja pod kątem zgodności z RODO projektów umów powierzenia danych osobowych, klauzul informacyjnych, regulaminów, polityk i innych dokumentów z obszaru ochrony danych osobowych;
   e) współpraca z organem nadzorczym;
   f) pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz dla osób, których dane są przetwarzane w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach,
   g) szkolenie nowych pracowników OPEC z zakresu ochrony danych osobowych;
   h) współdziałanie z ADO w procesach analizy ryzyka dla obszaru związanego z przetwarzaniem i ochroną danych osobowych
   i) zapewnienie obsługi zgłoszeń zdarzeń z udziałem danych osobowych, wsparcie administratora w ocenie incydentu oraz prowadzenie Rejestru naruszeń ochrony danych osobowych;
   j) udzielanie wyjaśnień i wsparcia w sprawach dotyczących ochrony danych osobowych w OPEC;
   k) prowadzenie Rejestru Czynności Przetwarzania Danych oraz zbiorczego Rejestru Kategorii Czynności Przetwarzania Danych
2. Aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać IOD odpowiada w szczególności za:
   a. sporządzanie analizy ryzyka dla zidentyfikowanych zagrożeń dla procesu przetwarzania danych osobowych;

b. opracowanie i wdrożenie polityki ochrony danych osobowych;
c. określenie częstotliwości dokonywania aktualizacji przedmiotowej polityki. Tym samym korzystając z posiadanych kompetencji IDO ustanawia, że przegląd będzie realizowany co najmniej raz w roku lub każdorazowo w przypadku istotnych zmian w strukturze organizacyjnej lub zakresie realizowanych zadań;
d. podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie;
e. przejrzyste, terminowe i właściwe i właściwe informowanie osób, których dane przetwarza o wszystkich okolicznościach przetwarzania oraz o przysługującym im prawach;
f. organizowanie administrowania danymi oraz określenie właściwych sposobów zabezpieczania danych osobowych;
g. podejmowanie w porozumieniu z ADO odpowiednich działań w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia przetwarzania danych osobowych, w tym w szczególności w przypadku konieczności jego niezwłocznego zgłoszenia organowi nadzorczemu (PUODO) - bez zbędnej zwłoki – nie później niż w terminie 72 godzin (art. 33 RODO);
h. przeprowadzenie analizy ryzyka procesu przetwarzania danych osobowych w formie zgodnej z przyjętą metodologią analizy ryzyka, pod kątem utraty poufności, dostępności i integralności. Przedmiotowa analiza wykonywana jest nie rzadziej niż raz w roku lub na skutek istotnych zamian organizacyjnych, czy też zmian zakresu wykonywanych zadań przez OPEC. Instrukcja postępowania w zakresie przeprowadzania ogólnej oceny ryzyka czynności przetwarzania oraz oceny skutków dla ochrony danych osobowych w OPEC Spółka z o.o., w Gdyni stanowi **załącznik nr 5 do niniejszej Polityki Ochrony Danych Osobowych;**
i. dokonywanie oceny ryzyka naruszenia praw lub wolności osób fizycznych, a gdy ryzyko to jest wysokie, oceny skutków przetwarzania dla ochrony danych osobowych (art. 35 RODO) w konsultacji z ADO;
j. określenie w postępowaniach zgodnych z p.z.p. i zawieranych umowach wymagań w zakresie projektowania prywatności w zamawianych produktach i usługach cyfrowych;
k. ustalanie zgodnego z celem i przepisami dotyczącymi archiwizacji okresu przetwarzania danych osobowych oraz ich usuwanie, gdy cel przetwarzania został zrealizowany i upłynął termin przechowywania. Obowiązek ten dotyczy także danych osobowych przetwarzanych w systemie elektronicznym;
l. przestrzeganie zasad i warunków udostępniania, a także wykorzystywania danych osobowych należących do innego administratora;
m. konsultacje w sprawie doboru podmiotów przetwarzających dane na rzecz OPEC, w trakcie których ADO określa wymagania w zakresie warunków przetwarzania w stosunku do podmiotów przetwarzających, zawiera z nimi stosowne umowy powierzenia danych osobowych;
n. prowadzenie rejestru umów powierzenia.

Rozdział VII
Kierownik komórki organizacyjnej

§ 11

1. Kierownik komórki organizacyjnej OPEC odpowiedzialny jest za ochronę danych osobowych w podległej jemu strukturze organizacyjnej.
2. Do obowiązków kierownika komórki organizacyjnej należy w szczególności:
   a) określenie na poziomie zarządzanej komórki katalogu czynności przetwarzania danych osobowych
   b) ustalenie i aktualizowanie indywidualnych zakresów czynności pracowników

zatrudnionych przy przetwarzaniu danych, w szczególności poprzez określenie odpowiedzialności za ochronę danych osobowych – w stopniu odpowiednim do zadań pracownika uczestniczącego w operacjach przetwarzania danych;

c) składanie wniosków o nadanie (modyfikację, odebranie) uprawnień do przetwarzania danych osobowych – wzór upoważnienia stanowi **załącznik nr 4 do Polityki Ochrony Danych Osobowych**- dla podległych pracowników
d) kierownik działu zasobów ludzkich odpowiada za prowadzenie i bieżące aktualizowanie ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór Rejestru ewidencji osób upoważnionych stanowi **złącznik nr 6. do Polityki Ochrony Danych Osobowych.**
e) każdorazowo przy planowaniu powierzenia danych osobowych, przedłożenia IOD projektu umowy/porozumienia powierzenia danych. Przedmiotowy projekt powinien być przedstawiony odpowiednio wcześnie, aby umożliwić IOD zajęcie stanowiska w sprawie.
f) bieżący nadzór nad funkcjonowaniem ustanowionych zabezpieczeń i przestrzeganiem zasad przetwarzania danych osobowych, określonych w niniejsze Polityce ODO, ze szczególnym uwzględnieniem prowadzenia i aktualizowania właściwych rejestrów;
g) przeprowadzenie szkolenia stanowiskowego dla pracownika z uwzględnieniem przyjętych zasad ochrony danych osobowych wynikających z niniejszej Polityki ODO;
h) zapewnienie ochrony tzw. danych niechcianych (dane nadmiarowe, niewymagane, dostarczone omyłkowo) poprzez odnotowanie ich w Rejestrze zdarzeń nieuprawnionego przetwarzania danych osobowych – wzór Rejestru zdarzeń nieuprawnionego przetwarzania danych osobowych stanowi **załącznik nr 8 do Polityki Ochrony Danych Osobowych**. Rejestr ten prowadzi kierownik komórki organizacyjnej. Dane osobowe będące przedmiotem niezamierzonego - nieuprawnionego przetwarzania – w zależności od możliwości administratora powinny bezzwłocznie zostać zwrócone, zanonimizowane lub usunięte.

Rozdział VIII
Osoba upoważniona do przetwarzania danych

§ 12

1) Może przetwarzać dane osobowe wyłącznie w zakresie ustalonym przez ADO w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków.
2) Zobowiązana jest do przestrzegania zasad przetwarzania danych osobowych w Okręgowym Przedsiębiorstwie Energetyki Cieplnej Spółka z o.o. w Gdyni załącznik nr 4 do Polityki ODO
3) Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Dochowanie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
4) Zapoznaje się z przepisami o ochronie danych osobowych oraz głównymi postanowieniami niniejszej „Polityki", jak też regulaminami i zarządzeniami odnoszącymi się do bezpieczeństwa informacji obowiązującymi w OPEC.
5) Jest zobowiązana do złożenia pisemnego oświadczenia o zachowaniu poufności danych osobowych i przestrzegania zasad i procedur określonych niniejszą Polityką ODO przez cały okres zatrudnienia oraz zachowania poufności danych osobowych po ustaniu okresu zatrudnienia. Treść oświadczenia jest zintegrowana z dokumentem Upoważnienia do przetwarzania danych osobowych (Załącznik nr3. do Polityki ODO).
6) Korzysta z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń systemu, oprogramowania i nośników.
7) Zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym w tym w szczególności w okresach świadczenia pracy poza obszarem administrowanym OPEC;
8) Zgłasza wszelkie zdarzenia dotyczących naruszenia ochrony danych osobowych kierownikowi komórki organizacyjnej oraz do IDO i ASI zgodnie z Instrukcją postępowania

w sytuacji naruszenia ochrony danych osobowych w OPEC w Gdyni – załącznik nr 8 do Polityki ODO.

Rozdział IX
Środki techniczne i organizacyjne służące zapewnieniu bezpieczeństwa procesowi przetwarzania danych

§ 13

1. Środki techniczne i organizacyjne stosowane są w celu zapewnienia i poprawy bezpieczeństwa danych osobowych przetwarzanych w OPEC, a tym samym ograniczenia ryzyka naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane.
2. Środki techniczne i organizacyjne, które zostały wdrożone w OPEC są efektem przeprowadzonej analizy ryzyka i zagrożeń dla bezpieczeństwa procesów przetwarzania informacji i danych osobowych.
3. Ogólny zapis środków technicznych i organizacyjnych oraz szczegółowe informacje dotyczące poszczególnych zabezpieczeń znajdują się w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, która stanowi **załącznik nr 9 do Polityki Ochrony Danych Osobowych** oraz Instrukcji postępowania z kluczami do pomieszczeń biurowych, która stanowi **załącznik nr 11 do Polityki Ochrony Danych Osobowych**..

§ 14

1. Poza środkami organizacyjnymi, o których mowa w Instrukcji, zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, na zabezpieczenia o charakterze organizacyjnym składają się:
   1) Polityka ochrony danych osobowych wraz załącznikami
   2) Środki o charakterze osobowym, do których zalicza się:
      a) obowiązek złożenia zobowiązania w formie oświadczenia przez wszystkich pracowników jednostki o zachowaniu poufności danych osobowych, do których przetwarzania zostali upoważnieni,
      b) system szkoleń wszystkich użytkowników z zakresu:
         - przepisów i procedur dotyczących ochrony danych,
         - sposobów ochrony danych przed osobami postronnymi i procedur udostępniania danych osobom, których te dane dotyczą,
         - obowiązków osób upoważnionych do przetwarzania danych osobowych,
         - odpowiedzialności za naruszenie obowiązków z zakresu ochrony danych osobowych..

Rozdział X
Infrastruktura przetwarzania danych osobowych

§ 15

Infrastrukturę przetwarzania danych osobowych tworzą budynki i pomieszczenia, systemy informatyczne oraz pozostałe aktywa będące nośnikami danych wykorzystywanych przez OPEC.

§ 16

ASI wraz z kierownikami komórek organizacyjnych dokonuje inwentaryzacji zasobów wykorzystywanych w procesie przetwarzania informacji (w tym osobowych) podczas przeprowadzania analizy ryzyka w zakresie Zarządzania Systemem Bezpieczeństwa Informacji. Więcej na ten temat zawiera Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, oraz Procedura Pracy Zdalnej i przetwarzania danych osobowych poza obszarem administrowania.

Rozdział XI
Pozostałe zasady bezpiecznego przetwarzania danych osobowych

§ 17

1. Szczególnej staranności wymaga wykonywanie pracy przez pracowników poza siedzibą jednostki. Dotyczy to zarówno pracy zdalnej w systemach, jak i przy wykorzystaniu dokumentacji papierowej.
2. Kierownik komórki organizacyjnej nadzoruje przemieszczanie dokumentów i innych nośników zawierających dane osobowe, niezależnie od częstotliwości i charakteru tych operacji. Zaleca się prowadzenie rejestru udostępnień i zwrotów dokumentów i innych nośników wykorzystywanych podczas pracy poza siedzibą jednostki organizacyjnej.

§ 18

Zasady zdalnego dostępu do systemów informatycznych oraz użytkowania sprzętu poza siedzibą Zarządu zostały opisane w Instrukcji pracy zdalnej. Dokument znajduje się w INTRANECIE na stronie głównej w folderze INFORMATYKA Praca zdalna w OPEC

§ 29

1. Administrator określi w postaci instrukcji pracy zdalnej warunki i zasady planowania, monitorowania oraz rozliczania pracy zdalnej, w tym nadzorowania danych osobowych przetwarzanych poza obszarem administrowania OPEC.
2. Regulamin, przywołany w ust. 1 zawiera wzory upoważnień i oświadczeń niezbędnych do zapewnienia bezpiecznego procesu przetwarzania danych osobowych w warunkach domowych.

Rozdział XII
Przeglądy okresowe, zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych

§20

1. ADO zaleca przeprowadzenie raz w roku przeglądu przetwarzania danych osobowych w zbiorach pod kątem celowości i zasadności ich dalszego przetwarzania, przechowywania. Pracownicy przetwarzający dane osobowe są zobowiązani do współpracy z osobą dokonującą przeglądu i wskazania jej danych osobowych, czynności przetwarzania, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania lub brak ich adekwatności do realizowanego celu.
2. ADO może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd może nastąpić w sytuacji zmian organizacyjnych u administratora danych, jak i w każdej innej sytuacji, która w ocenie ADO lub IOD będzie wymagała przeprowadzenia takiego przeglądu.
3. Przegląd przeprowadza IOD wspólnie z kierownikami jednostek organizacyjnych, którzy przetwarzają dane osobowe.

Rozdział XIII
Udostępnianie danych osobowych

§ 21

Udostępnianie danych osobowych policji, sądom, prokuraturze oraz pozostałym organom ścigania i wymiaru sprawiedliwości może nastąpić w związku z prowadzonym przez te organy postępowaniem, zgodnie z przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019r. poz. 125).

Rozdział XIV
Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

§ 22

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art.52 Kodeksu pracy.

Rozdział XV
Postanowienia końcowe

§ 23

1. Każda osoba upoważniona do przetwarzania danych osobowych przed dopuszczeniem do przetwarzania danych, zobowiązana jest do zapoznania się z niniejszym dokumentem oraz wraz z upoważnieniem podpisać stosowne oświadczenie.
2. Zaleca się prowadzenie ewidencji i rejestrów stanowiących załączniki do niniejszej Polityki ODO w wersji elektronicznej.

Załączniki (wzory dokumentów):

1. Rejestr czynności przetwarzania danych osobowych;
2. Rejestr kategorii czynności przetwarzania;
3. Procedura nadawania, zmiany i wycofania upoważnień i uprawnień do przetwarzania danych osobowych;
4. Zasady przetwarzania danych osobowych w OPEC Spółka z o.o. w Gdyni;
5. Instrukcja postępowania w zakresie przeprowadzania ogólnej oceny ryzyka czynności przetwarzania oraz oceny skutków dla ochrony danych osobowych w OPEC Spółka z o.o. w Gdyni;
6. Ewidencja upoważnionych - wzór;
7. Rejestr zdarzeń nieuprawnionego przetwarzania danych osobowych;
8. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w OPEC Spółka z o.o. w Gdyni.
9. Instrukcja Zarządzania Systemami Informatycznymi Służącymi Do Przetwarzania Danych Osobowych Dla OPEC Spółka z o.o. w Gdyni,
10. Zasady przetwarzania danych osobowych w systemach monitoringu wizyjnego obowiązujące w OPEC Spółka z o.o. w Gdyni.
11. Instrukcja postępowania z kluczami do pomieszczeń biurowych