POLITYKA BEZPIECZEŃSTWA

w sprawie ochrony danych osobowych w:

Ogólnopolski Związek Zawodowy Oficerów i Marynarzy
Plac Kaszubski 8, 81-350 Gdynia

Celem Polityki bezpieczeństwa przetwarzania danych osobowych jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

Ogólnopolski Związek Zawodowy
Oficerów i Marynarzy
PRZEWODNICZĄCY

Henryk Piątkowski

15.06.2018

/zatwierdzam do stosowania, podpis, data/

I. Definicje

§1

1. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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. **USTAWA** - Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000)
3. **Rozporządzenie MSWiA** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
4. **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
5. **zbiór danych osobowych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
6. **przetwarzanie danych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
7. **administrator danych** – Ogólnopolski Związek Zawodowy Oficerów i Marynarzy Plac Kaszubski 8, 81-350 Gdynia
8. **załącznik nr** … - jeżeli w treści Polityki bezpieczeństwa występuje zwrot „załącznik nr …" oznacza to załącznik do Polityki bezpieczeństwa, który stanowi jego integralną część
9. **osoba upoważniona do przetwarzania danych** (nazwa skrócona: **użytkownik)** – osoba upoważniona przez administratora danych do przetwarzania danych osobowych. Osobą taką jest pracownik administratora danych na podstawie pisemnego upoważnienia (wzór załącznik nr 4), wykaz użytkowników zawiera załącznik nr 2 lub pracownicy innego podmiotu, któremu dane osobowe zostały powierzone na podstawie „umowy o powierzeniu danych" (wzór załącznik nr 9).
10. **Instrukcja zarządzania** (nazwa skrócona: **Instrukcja)** – dokument o nazwie „Instrukcja zarządzania systemem informacji przetwarzającym dane osobowe w: Ogólnopolski Związek Zawodowy Oficerów i Marynarzy Plac Kaszubski 8, 81-350 Gdynia
11. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
12. **system tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

13. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
14. **zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie: zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści (wzór załącznik nr 7),
15. **osoba nieuprawniona** – rozumie się przez to osobę nie zatrudnioną przy gromadzeniu lub przetwarzaniu danych (z wyłączeniem osoby uprawnionej do ich przeglądania i przetwarzania na mocy odrębnych przepisów).
16. **dane wrażliwe** - dane określające poglądy polityczne, przekonania religijne, pochodzenie rasowe, orientację seksualną, przynależność do związków zawodowych, dotyczące wyroków skazujących lub naruszeń prawa a także dane zdrowotne, biometryczne lub genetyczne.
17. **umowa powierzenia danych** – umowa pomiędzy administratorem danych a innym podmiotem, w którym określa się cel i zakres powierzonych danych. Tym celem najczęściej będzie przeniesienie części procesów przetwarzania danych osobowych poza siedzibę firmy, np. hosting, obsługa kadrowo-księgowa, prawna lub obsługa informatyczna. (wzór załącznik nr 9)
18. **konto e-mail administratora danych osobowych** – konto e-mail do obsługi spraw związanych z ochroną danych osobowych. Nazwa konta oraz wyznaczenie osoby do obsługi tego konta zawiera załącznik nr 14.

II. Przepisy ogólne

§ 2

1) Dane osobowe mogą być przetwarzane:

   a) w systemach informatycznych,
   b) systemem tradycyjnym: w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych w postaci papierowej.

2) Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy spełniony jest, co najmniej jeden z wymienionych poniżej warunków:

   a) osoba, której dane dotyczą, wyrazi zgodę na przetwarzanie danych, zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, lecz musi wyraźnie dotyczyć przetwarzania danych; wzór zgody osoby na przetwarzanie jej danych osobowych stanowi załącznik nr 7,

   b) na przetwarzanie danych zezwalają odrębne przepisy prawa,

   c) przetwarzanie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia koniecznych działań przed zawarciem umowy,

   d) przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

   e) przetwarzanie danych jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych lub osób trzecich, którym są przekazywane te dane, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów administratora danych powinna być dokonywana indywidualnie w każdej sytuacji.

Podstawy prawne przetwarzania danych osobowych w RODO

Przepis RODO	Podstawa prawna przetwarzania danych osobowych /dane osobowe – zwykłe/
Art. 6 ust. 1 pkt a)	Zgoda osoby, której dane dotyczą
Art. 6 ust. 1 pkt b)	Realizacja umowy lub żądanie jej zawarcia przez osobę
Art. 6 ust. 1 pkt c)	Obowiązek prawny ciążący na administratorze danych
Art. 6 ust. 1 pkt d)	Ochrona żywotnych interesów osoby
Art. 6 ust. 1 pkt e)	Zadanie jest realizowane w interesie publicznym
Art. 6 ust. 1 pkt f)	Prawnie uzasadniony cel realizowany prze administratora danych

3) Wykaz zbiorów danych osobowych zewidencjonowany u administratorach danych zawiera załącznik nr 15

4) Wykaz pomieszczeń i stref w których przetwarza się dane osobowe zawiera załącznik nr 3

III. Obowiązki administratora danych

§ 3

1) W przypadku zbierania danych osobowych od osoby, której one dotyczą należy poinformować tę osobę o:

   a) o istnieniu zbioru jej danych osobowych,
   b) o adresie swojej siedziby i pełnej nazwie,
   c) o celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
   d) o prawie wglądu do swoich danych oraz ich poprawiania,
   e) o prawie „do bycia zapomnianym"
   f) o dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Wzór informacji, o której mowa w ust. 1 stanowi załącznik nr 12

Obowiązek informowania określony w § 3 spoczywa na użytkownikach, którzy zobowiązani są do jego należytego wykonywania.

§ 4

1) Na administratorze danych ciąży obowiązek ochrony integralności i poprawności przetwarzanych informacji, szczególnie jest on obowiązany:

   a) przetwarzać je zgodnie z prawem,
   b) zbierać dane dla oznaczonych, zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami,
   c) gromadzić dane merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   d) przechowywać je w postaci umożliwiającej identyfikację osób, których dotyczą nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2)Administrator danych jest odpowiedzialny za to, komu powierza dane osobowe oraz nadzór nad przestrzeganiem RODO przez te podmioty. Najlepiej jest zawrzeć „umowę powierzenia danych" z takim podmiotem /wzór załącznik nr 9/. W tabeli poniżej przedstawiono obowiązki podmiotu oraz ich podstawy prawne, które powinny zostać zawarte w tej umowie:

Przepis RODO	Obowiązki podmiotu, któremu powierzamy dane osobowe
Art. 28 ust. 1	Wdrożenie zabezpieczeń technicznych i organizacyjnych zgodnych z RODO
Art. 28 ust. 2	Podpowierzenie danych innemu podmiotowi tylko za pisemną zgodą administratora danych
Art. 28 ust. 3	W umowie należy określić: przedmiot, czas trwania, charakter i cel przetwarzania oraz rodzaj danych i kategorie osób

Art. 28 ust. 4	Podmiot odpowiada za działania lub zaniechania innych podmiotów, którym podpowierzono dane osobowe.
Art. 37 ust. 41	Wyznacza inspektora ochrony danych, jeżeli powierzone dane wymagają powołania takiej osoby.

3) Do obowiązków administratora danych osobowych należy również zebranie oświadczeń, (wzór załącznik nr 6) od swoich pracowników, niezbędnych do prawidłowego wykonywania obowiązków tej placówki jako zakładu pracy i innych obowiązków wynikających z przepisów prawa.

4) Do obowiązków administratora danych należy wydanie imiennych upoważnień do przetwarzania danych osobowych dla swoich pracowników (wzór załącznik nr 4).

5) Prowadzenia postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych (wzór załącznik nr 13)

Zgodnie z art. 33 ust. 1 RODO administrator danych ma obowiązek zgłaszania incydentów naruszenia ochrony danych osobowych do Urzędu Ochrony Danych Osobowych (skrót: UODO)– w miarę możliwości bez zbędnej zwłoki, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego UODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

§ 5

1) Administrator danych ma obowiązek powołać IOD – Inspektora Danych Osobowych. W przypadku gdy:

   a) jest organem lub podmiotem sektora publicznego
   b) prowadzi regularne i systematyczne monitorowanie osób na dużą skalę
   c) główna działalność administratora danych polega na przetwarzaniu danych wrażliwych na duża skalę

2) Administrator danych ma obowiązek prowadzenia Rejestru Czynności Przetwarzania gdy:

   a) zatrudnia powyżej 250 osób
   b) przetwarzanie stwarza ryzyko naruszenia praw i wolności osób, których dane dotyczą i nie ma charakteru sporadycznego
   c) przetwarzane są dane osobowe szczególnej kategorii (dane wrażliwe)
   d) przetwarza się dane osobowe dotyczące wyroków skazujących lub naruszeń prawa

3) W przypadku wprowadzenia monitoringu wizyjnego administrator danych ma obowiązek poinformować o tym fakcie swoich pracowników. Informację taką można umieścić w oświadczeniach dla pracownika (załącznik nr 5) lub w formie osobnego pisma, które pracownik powinien podpisać.

IV. Prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.

§ 6

1) Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

   a) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
   b) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
   c) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w powszechnie zrozumiałej formie treści tych danych,
   d) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
   e) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępnione,
   f) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane,
   g) prawo „do bycia zapomnianym". Prawo to może być realizowane, gdy spełniony jest jeden spośród następujących warunków:

      - dane nie są już dłużej niezbędne do realizacji celu, w jakim zostały zebrane lub są przetwarzane;
      - podmiot danych wycofał zgodę na przetwarzanie jego danych osobowych oraz nie istnieją podstawy prawne, aby mimo tego kontynuować przetwarzanie;
      - podmiot danych sprzeciwia się przetwarzaniu oraz nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania, lub
      - podmiot danych sprzeciwia się przetwarzaniu jego danych osobowych na potrzeby i w zakresie marketingu bezpośredniego (w tym profilowania);
      - przetwarzanie w inny sposób nie jest lub nie było zgodne z RODO lub innymi przepisami prawa;
      - dane osobowe zostały zebrane w nawiązaniu do oferowania bezpośrednio osobom poniżej 16 lat usług społeczeństwa informatycznego (np. e-handel, portale społecznościowe)

   h) Poniżej podstawy prawne praw osób, których dane osobowe mogą być przetwarzane przez administratora danych:

Podstawa prawna	Prawo osób
Art. 7 RODO	Prawo do cofnięcia zgody
Art. 15 RODO	Prawo dostępu do danych
Art. 16 RODO	Prawo do poprawiania danych

Art. 17 RODO	Prawo do bycia zapomnianym (usunięcia danych)
Art. 18 RODO	Prawo do ograniczenia przetwarzania
Art. 20 RODO	Prawo do przeniesienia danych
Art. 21 RODO	Prawo do sprzeciwu wobec przetwarzania danych

Administrator danych ma 30 dni na odpowiedź na złożony wniosek dotyczący praw osoby wobec przetwarzania jej danych osobowych.

V. Zabezpieczenie fizyczne zbiorów danych osobowych

§ 7

1) W przypadku gdy obiekty budowlane wykazane w załączniku nr 3, w których przetwarza się dane osobowe są objęte monitoringiem wizyjnym oraz systemem alarmowym, powinny podlegać okresowym przeglądom technicznym.
2) Drzwi do pomieszczeń w których przetwarza się dane wyposażone są w zamki i klucze umożliwiające ich zamykanie.
3) Szafki w których przechowuje się papierowe dane osobowe wyposażone są w zamki i klucze umożliwiające ich zamykanie.
4) Systemy informatyczne posiadają awaryjne podtrzymanie napięcia elektrycznego w postaci UPS-ów lub baterii.
5) W obiektach dostępna jest niszczarka dokumentów
6) W przypadku gdy firma posiada swoje oddziały poza siedzibą firmy, które łączą się z serwerem danych osobowych w siedzibie firmy, dla zapewnienia bezpieczeństwa tego połączenia wymagany jest szyfrowany kanał IPSEC VPN.
7) Wprowadza się listę kontrolną /załącznik nr 11/ do przetestowania w jakim stopniu stanowisko komputerowe jest podatne na ryzyka wystąpienia incydentu. Kontrolę stanowisk powinna wykonać osoba pełniąca rolę informatyka w firmie /lub pracownik firmy zajmującej się opieką informatyczną/. Podsumowanie kontroli ze wszystkich stanowisk powinno być przesłane na adres as@psu-pl.org. w celu zapoznania się Administratora danych z jej wynikami i ewentualnym podjęciu dalszych działań. Ustala się dokonanie takiej czynności co najmniej raz w roku.

VI. Zabezpieczenie organizacyjne zbiorów danych osobowych

§ 8

1) Administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem bez podstaw prawnej, zmianą lub utratą, uszkodzeniem lub zniszczeniem.

2) Szczegółowy opis procedur realizujących poszczególne zadania zawiera załącznik nr 1.

§ 9

1) Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej powinien być zapoznany z Instrukcją zarządzania.
   Za dopełnienie tego obowiązku odpowiada administrator danych.
2) Po zapoznaniu się z dokumentacją użytkownik podpisuje oświadczenia o zapoznaniu się z dokumentacją i jej zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w niej zasad ochrony danych osobowych. (wzór załącznik nr 5)
3) Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.
4) Na podstawie zakresu obowiązków użytkownika wynikających z nałożonych na użytkownika zadań wydaje się imienne upoważnienie do przetwarzania danych osobowych wraz z wyszczególnieniem zbiorów, których to upoważnienie dotyczy. Wzór takiego upoważnienia zawiera załącznik nr 4

§ 10

1) Do obsługi zgłoszeń związanych z tematyka ochrony danych osobowych należy wyznaczyć osobę, która będzie obsługiwać określono konto e-mail. Osoba ta może być pracownikiem administratora danych lub pracownikiem podmiotu zewnętrznego. Do zadań tej osoby należy:
   a) sprawdzanie wiadomości na koncie e-mail i przekazywanie do odpowiednich komórek firmy w zależności od ich treści,
   b) prowadzenia rejestru incydentów związanych z ochroną danych osobowych /wzór załącznik nr 13/

Dla celów dowodowych zaleca się prowadzenie drukowanej wersji wiadomości dotyczących ochrony danych osobowych nadesłanych na to konto e-mail.
Wyznaczenie takiej osoby powinno nastąpić w formie pisemnej /wzór załącznik nr 14/

VII. Odpowiedzialność za naruszenie Polityki bezpieczeństwa.

§ 11

1) Obowiązki i odpowiedzialność poszczególnych użytkowników w zakresie ochrony i zabezpieczania danych osobowych powinien określać indywidualny zakres czynności tej osoby oraz oświadczenie, które stanowi załącznik nr 5.

2) Wobec osoby, która w przypadku naruszenia zasad ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania polegającego na powiadomieniu administratora danych zgodnie z określonymi procedurami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

VIII. Zmiany Polityki Bezpieczeństwa.

§ 12

1) Wszelkie zmiany w powyższej Polityki bezpieczeństwa wprowadzane przez administratora danych skuteczne są wobec wszystkich osób, których dotyczą, z chwilą ich doręczenia tym osobom na piśmie. Kolejne zmiany dokumentu powinny być oznaczone kolejnym numer wersji i datą umieszczonym w stopce dokumentu.

2) Administrator danych zobowiązany jest aktualizowania dokumentacji ochrony danych osobowych. Zaleca się przeprowadzenie przynajmniej raz w roku audytu tej dokumentacji w ramach sprawdzeń zgodności z RODO przez podmioty zajmujące się tą tematyką.

3) Oryginały aktualnej dokumentacji ochrony danych osobowych będą przechowywane w Centrali OZZOiM Plac Kaszubski 8, Gdynia.

IX. Moc obowiązująca

§ 13

1) Niniejsza Polityka bezpieczeństwa wraz z Instrukcją zarządzania zostaje wprowadzona zarządzeniem 3/2018 Przewodniczącego OZZOiM z dnia 15 czerwca 2018r.

2) W sprawach nieuregulowanych w Polityce bezpieczeństwa mają zastosowanie obowiązujące przepisy dotyczące ochrony danych osobowych.