# Polityka Bezpieczeństwa w Zakresie Ochrony Danych Osobowych w Izbie Rzemieślniczej w Opolu ul. Katowicka 55 45-061 Opole

Opole, 25 maj 2018

## SPIS TREŚCI

1 Wstęp....3

2 Ocena skutków (analiza ryzyka)....7

3 Udostępnianie danych....9

4 Osoby przetwarzające dane....10

5 Katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie....11

6 Prawa osób, których dane są przetwarzane....12

7 OBSZAR IZBY, ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE....13

8 ARCHIWIZOWANIE DANYCH....14

9 ZBIORY DANYCH....14

10 SPRAWOZDANIE Z FUNKCJONOWANIA SYSTEMU OCHRONY DANYCH OSOBOWYCH....15

11 Postanowienia końcowe....15

# 1 WSTĘP

Izba Rzemieślnicza w Opolu (dalej Izba) jest organizacją samorządu gospodarczego rzemiosła działającą w oparciu o ustawę z dnia 22 marca 1989 r. o rzemiośle (Dz.U. 1989 Nr 17 poz. 92 z późniejszymi zmianami).

Zadaniem Izby jest ochrona praw i reprezentowanie członków wobec organów administracji publicznej oraz innych organizacji i instytucji, rozwijanie działalności społeczno-zawodowej rzemiosła, udzielanie swym członkom pomocy instruktażowej i doradczej oraz przeprowadzanie egzaminów kwalifikacyjnych czeladniczych i mistrzowskich, organizacja szkoleń branżowych oraz pozostałych pozaszkolnych form edukacji w tym szkoleń związanych głównie z rozwijaniem własnych zainteresowań oraz doskonaleniem zawodowym.

Beneficjentami Izby są firmy sektora MSP, członkowie organizacji samorządu gospodarczego rzemiosła, instytucje państwowe i samorządowe, a także osoby fizyczne pragnące podnieść swoje kwalifikacje lub chcące założyć własną działalność gospodarczą, beneficjenci realizowanych przez Izbę projektów współfinansowanych lub finansowanych ze środków Unii Europejskiej.

Polityka Ochrony Danych Osobowych jest dokumentem opisującym cele, zasady ochrony i sposoby przetwarzania danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO), dostosowując odpowiednie środki techniczne i organizacyjne, z uwzględnieniem potencjalnych ryzyk i jest w szczególności przeznaczona dla pracowników Izby przetwarzających dane osobowe.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

Administratorem danych Osobowych jest Izba Rzemieślnicza w Opolu z siedzibą ul. Katowicka 55, 45-061 Opole, NIP 7540340252, wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000030157. Administratorem danych osobowych mogą być również inne instytucje, z którymi Izba współpracuje przy realizacji programów finansowanych ze środków Unii Europejskiej.

**DEFINICJE**

**Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot (**Dyrektor Izby Rzemieślniczej w Opolu**), który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

**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)

**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, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego tożsamość tej osoby fizycznej.

**Zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów.

**System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

**System tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze.

**Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

**Administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi.

**Identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

**Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

**Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

**Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

**Anonimizacja**- zmiana danych osobowych w wyniku, której dane te tracą charakter danych osobowych.

**Zgoda osoby, której dane dotyczą** - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

**Ocena skutków w ochronie danych** - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych, jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

**Podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

**Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

**Podmiot przetwarzający (Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

**Inspektor Ochrony Danych (IOD)** - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania, jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

**Pseudonimizacja** - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

**Szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej

identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

**Profilowanie** – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

**Naruszenie ochrony danych osobowych** - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

## ZAKRES I CEL POLITYKI BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Polityka ma zastosowanie do:

- danych osobowych przetwarzanych w zbiorach danych tradycyjnych pisemnych, w szczególności w kartotekach, wykazach oraz zestawieniach, rejestrach w systemach informatycznych, a także w przypadku przetwarzania danych poza zbiorem lokalnym za pomocą komputera przenośnego wspomagającego pracę Izby,
- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych (Windows, Microsoft Office, Open Office, Optima, HSI, SIO, Płatnik itp.) oraz papierowych, w których przetwarzane są dane osobowe;
- danych osobowych powierzonych na podstawie zawartych umów;
- wszystkich pomieszczeń, w których są lub będą przetwarzane dane osobowe;
- wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, osób zatrudnionych na podstawie umów cywilnoprawnych i innych osób mających dostęp do danych osobowych;
- podmiotów którym dane osobowe są przekazywane w celach wynikających z zawartych umów o współpracę.

Główne cele Polityki:

- zapewnienie spełnienia wymagań prawnych;
- ochrona systemów przetwarzania przed nieuprawnionym dostępem bądź zniszczeniem;
- podnoszenie świadomości w zakresie ochrony danych osobowych;
- minimalizacja ryzyka utraty informacji.

## 2 OCENA SKUTKÓW (ANALIZA RYZYKA)

1. Dane w Izbie przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:

- 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) (Dz.U.UE.L.2016.119.1) – dalej RODO
- Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (z późniejszymi zmianami) i przepisów wykonawczych z nią związanych,
- Ustawy o rzemiośle z dnia 22 marca 1989 r. - (t.j. Dz. U. z 2016 r. poz. 1285, z 2017 r. poz. 60),
- Ustawa z dnia 15 kwietnia 2011 w sprawie systemu informacji oświatowej (t.j. z 2016 r. poz. 1927, 1984, z 2017 r. poz. 60, 777, 949).
- Rozporządzenia Ministra Edukacji Narodowej z dnia 10 stycznia 2017 r. w sprawie egzaminu czeladniczego, egzaminu mistrzowskiego oraz egzaminu sprawdzającego, przeprowadzanych przez komisje egzaminacyjne izb rzemieślniczych (Dz.U. 2017 poz. 89 z zmianą Dz.U. 2017 poz. 1607)
- Rozporządzenie MGiP z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy,
- Rozporządzenie MEN z dnia 11 stycznia 2012 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych,
- Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalania okoliczności i przyczyn wypadków przy pracy,
- Rozporządzenie Rady Ministrów z dnia 2 września 1997 r. w sprawie służby bhp,
- Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2017 r. poz. 1065).

2. Dane w Izbie są przetwarzane w celu realizacji działalności Izby w szczególności dane osobowe przetwarza się:

- dla celów rekrutacji pracowników do Izby
- dla zabezpieczania prawidłowego toku realizacji zadań Izby
- dla realizacji innych usprawiedliwionych celów i zadań Izby - z poszanowaniem praw i wolności osób powierzających w Izbie swoje dane
- wykonywania obsługi biurowej i organizacyjnej organów statutowych Izby.

- zarządzania danymi pracowników etatowych Izby i osób zatrudnionych w ramach umów cywilnoprawnych, zgodnie z odnośnymi uregulowaniami prawa
- przetwarzania danych osobowych związanych z realizacją projektów z udziałem wsparcia finansowego ze środków Unii Europejskiej, zgodnie z zasadami określonymi odrębnymi przepisami odnoszącymi się do poszczególnych „źródeł wsparcia" oraz danych osobowych pozyskiwanych w celu realizacji innych zadań statutowych Izby jak działania w obszarze przedsięwzięć szkoleniowo-oświatowych.
- przetwarzania danych osobowych związanych z obsługą Izby.

3. Realizując politykę dokłada się szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

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

4. Realizując politykę stosuje się odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:

- zabezpiecza dane uniemożliwiając pozyskanie ich osobie nieupoważnionej,
- zabraniem przez osobę nieuprawnioną,
- przetwarzaniem z naruszeniem ustawy,
- nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

5. Realizując politykę Izba dąży do systematycznego unowocześniania stosowanych środków ochrony tych danych. W szczególności Izba zapewnia środki ochrony danych pozwalające na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz innymi zagrożeniami wynikającymi z funkcjonowania systemu informatycznego.
6. Każdy pracownik posiadający dostęp do danych osobowych przechowywanych w wersji papierowej oraz w wersji elektronicznej składa oświadczenie na piśmie zawierające świadome zobowiązanie do przestrzegania zasad gromadzenia, przechowywania i przetwarzania danych osobowych w sposób zgodny z przepisami prawa i niniejszej Polityki bezpieczeństwa. Wzór oświadczenia pracownika stanowi załącznik do Polityki Bezpieczeństwa.
7. Niszczenie zbędnych danych lub ich zbiorów polega na trwałym, fizycznym zniszczeniu danych wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.

8. Osoby przetwarzające dane mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych.
9. Naruszanie przez zatrudnione w przyszłości osoby, w ramach stosunku pracy, procedur dostępu lub przetwarzania danych wykorzystywanych w Izbie w tym procedur niszczenia zbędnych danych traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającym konsekwencjami, z rozwiązaniem stosunku pracy włącznie.
10. Nadzór nad niszczeniem zbędnych danych odbywać się będzie przez Administratora lub w przypadku jego obecności przez osoby upoważnione do wykonania tej czynności.
11. Realizując politykę prowadzi się dokumentację opisującą sposób przetwarzania danych oraz środki ochrony tych danych. W skład tej dokumentacji wchodzą w szczególności:

- Polityka Bezpieczeństwa w Zakresie Ochrony Danych w Izbie Rzemieślniczej w Opolu wraz z załącznikami,
- Zarządzenia, instrukcje, wytyczne i polecenia służbowe określające zasady i procedury mające znaczenie dla ochrony danych wydawane przez Dyrektora Izby.

Analiza ryzyka stanowi załącznik do niniejszej Polityki Bezpieczeństwa w Zakresie Ochrony Danych Osobowych.

## 3 UDOSTĘPNIANIE DANYCH

1. Realizując politykę bezpieczeństwa udostępnia się dane przetwarzane w Izbie wyłącznie osobom/instytucjom do tego upoważnionym na mocy uregulowań wewnętrznych/zewnętrznych obowiązujących w tym zakresie.
2. Upoważnienie to wynika w szczególności z:
   - ✓ charakteru pracy wykonywanej na danym stanowisku pracy, lub dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy, lub odrębnego dokumentu zawierającego imienne upoważnienie dostępu do danych, własności baz danych.
3. Realizując politykę Administrator danych – Dyrektor Izby zapewnia wgląd i możliwość aktualizacji danych osobom fizycznym i prawnym będących dysponentami tych danych.
4. Dysponentami danych są podmioty, które powierzyły swoje dane Izbie w związku z realizacją celów działalności Izby.
5. Osoby niezatrudnione przy przetwarzaniu danych w tym dysponenci danych, mający interes prawny lub faktyczny w uzyskaniu dostępu do tych danych mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika Izby.

6. Dostęp do danych i ich przetwarzanie bez odrębnego upoważnienia administratora danych lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych o określonej kategorii.
7. W szczególności dostęp do danych mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, Wojskowe Służby Informacyjne, sądy powszechne, Najwyższa Izba Kontroli, Prezes Urzędu Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień - wszystkie ww. po okazaniu dokumentów potwierdzających te uprawnienia.
8. Dostęp do zbiorów danych wynikać może z zawartych umów o powierzenie.

## 4 OSOBY PRZETWARZAJĄCE DANE

1. Administrator Danych Osobowych (Dyrektor Izby) wyznacza osoby odpowiedzialne za bieżącą realizacje tej polityki na terenie Izby. W szczególności wyznaczeni są naczelnicy wydziałów, księgowa i zastępca dyrektora.
2. Dopuszcza się do przetwarzania wyłącznie osoby posiadające uprawnienia nadane przez ADO.
3. Administrator Danych Osobowych zapewnia nadzór nad prawidłowością dostępu do tych danych. Nadzór ten w szczególności realizowany jest poprzez ewidencjonowanie osób przetwarzających dane. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO - załącznik Ewidencja osób upoważnionych.
4. Administrator Danych Osobowych zapewnia zaznajomienie osób upoważnionych do dostępu do danych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Izbie.
5. Osoby wskazane w punkcie 4, zaznajamiane są z kwestiami wymienionymi w tym przepisie przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych, a także odpowiednio w trakcie trwania zatrudnienia w przypadku ich aktualizacji. Zaznajomienie osób upoważnionych do przetwarzania danych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Izbie może odbywać się w szczególności poprzez:
    - instruktaż na stanowisku pracy,
    - szkolenie wewnętrzne realizowane na terenie Izby
    - szkolenie zewnętrzne.

6. Osoby upoważnione przez Administratora Danych Osobowych do przetwarzania danych zostają zapoznane z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. Osoby te są poinformowane o obowiązku zachowania w tajemnicy przetwarzanych danych w Izbie.
7. Naruszanie przez upoważnione osoby lub podmioty bezpiecznego i zgodnego z prawem zasad przetwarzania danych, traktowane będzie jako naruszenie podstawowych norm i obowiązków wynikających z obowiązujących aktów normatywnych i skutkować będzie konsekwencjami wynikającymi 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.U.UE.L.2016.119.1) – dalej RODO.

# 5 KATALOG PODATNOŚCI I INCYDENTÓW ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU DANYCH OSOBOWYCH ORAZ SPOSÓB REAGOWANIA NA NIE.

Procedura niniejsza definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych).
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)

b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)

c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
   b. inicjuje ewentualne działania dyscyplinarne
   c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
   d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

## 6 PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Izba zapewnia podmiotom, których dane osobowe są przetwarzane w związku z realizacją celów Izby, realizację uprawnień gwarantowanych im przez obowiązujące przepisy prawa.

Osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacja celów Izby, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych ich korekty, o tym w jakim celu te dane są przetwarzane, a także prawo do dostępu do danych, możliwości ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, kontroli przetwarzania danych, do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych oraz prawo do wniesienia skargi do organu nadzorczego. Podanie danych jest dobrowolne.

## 7 OBSZAR IZBY, ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE

1. Opracowano i wdrożono politykę bezpieczeństwa przetwarzania danych osobowych.

2. Realizując politykę wyznacza się pomieszczenia, tworzące obszar, w którym przetwarzane są dane.

3. Zabezpieczenia danych osobowych przechowywanych w postaci papierowej:
   - Szafy i urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach.
   - Dane osobowe przetwarzane w formie papierowej przechowuje się w zamykanych szafach metalowych i niemetalowych wyposażonych w zamki uniemożliwiające dostęp osób niepowołanych, do których wydawane są za pokwitowaniem pojedyncze egzemplarze kluczy.
   - Jednostkami zbiorów danych osobowych gromadzonych i przetwarzanych w wersji papierowej są:
   - ✓ Segregatory zawierające teczki i podteczki, w których gromadzone są oryginalne dokumenty w formie kart papierowych;
   - ✓ Księgi wieczyste egzaminów czeladniczych i mistrzowskich,
   - ✓ Rejestry w postaci druku zwartego.
   - Pomieszczenia, w których zlokalizowane są szafy zamykane są na zamki, do których klucze wydawane są za pokwitowaniem odbioru osobom uprawnionym przez portiera w recepcji budynku.
   - Osoby dysponujące kluczami do szaf oraz do pomieszczeń obowiązane są do korzystania z dokumentów z wyłączeniem osób niepowołanych oraz ponoszą z tego tytułu odpowiedzialność służbową.
   - Zapasowe komplety kluczy do pomieszczeń przechowywane są w kasie pancernej Wydziału Administracyjno-Finansowego, ruch kluczy zapasowych podlega kontroli przez Naczelnika Wydziału Administracyjno-Finansowego.
   - Wykaz pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych wraz z wykazem pracowników upoważnionych do odbierania kluczy stanowi załącznik do Polityki Bezpieczeństwa.

4. Akta, dokumenty, rejestry, dyski, pen drivy, pieczątki i inne przedmioty służbowe są zabezpieczone przed nieuprawnionym dostępem osób postronnych. Opracowany został rejestr nośników pamięci.

5. Laptopy oraz inne urządzenie przenośne służbowe użytkowane w Izbie po zakończeniu pracy są zabezpieczone przed dostępem, a te do których dostęp posiada wyłącznie osoba je użytkująca – hasło otwierające komputer zmieniane cyklicznie raz w miesiącu i składające się z wielkich liter, małych liter cyfr i znaków specjalnych. Laptopy posiadają oprogramowanie antywirusowe z licencją ESET NOD32.

6. Klucze do pomieszczeń specjalnych, w których są przechowywane i archiwizowane dane wydawane są wyłącznie osobom upoważnionym do przetwarzania danych osobowych. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafce i mogą być wydawane w sytuacjach awaryjnych.

7. Administrator Danych Osobowych realizując Politykę Bezpieczeństwa może wprowadzać inne elektroniczne formy monitorowania dostępu do obszarów przetwarzania danych.
8. Zasady postępowania w przypadku naruszenia ochrony danych osobowych określa załącznik do Polityki Bezpieczeństwa.

## 8 ARCHIWIZOWANIE DANYCH

Administrator Danych Osobowych prowadzi Archiwum tradycyjne na obszarze Izby. Dokumenty przenoszone są do Archiwum nie rzadziej niż raz w roku.

## 9 ZBIORY DANYCH

1. W Izbie ADO realizując politykę sprawuje nadzór nad rodzajami oraz zawartością powierzonych zbiorów danych.
2. Wykaz zbiorów danych wraz ze wskazaniem struktury zbiorów danych, zawartości poszczególnych pól informacyjnych i powiązań miedzy nimi.
   - ✓ Nazwa zbioru: Uczestnicy szkolenia z zakresu bezpieczeństwa i higieny pracy

   Dane osobowe które będą przetwarzane: imię i nazwisko, data urodzenia, miejsce urodzenia
   - ✓ Nazwa zbioru: Uczestnicy szkolenia z zasad udzielania pierwszej pomocy przedmedycznej lub uczestnicy szkolenia z zasad ochrony przeciwpożarowej.

   Dane osobowe które będą przetwarzane: imię i nazwisko, data urodzenia, miejsce urodzenia, pesel.
   - ✓ Nazwa zbioru: Postępowanie wypadkowe, rejestr wypadków przy pracy

Dane osobowe które będą przetwarzane: imię i nazwisko, data urodzenia, miejsce urodzenia, pesel, adres zamieszkania, numer dowodu osobistego, imię ojca.

✓ Nazwa zbioru: Dokumentacja z zakresu bhp

Dane osobowe które będą przetwarzane: imię i nazwisko, data urodzenia, miejsce urodzenia.

## 10 SPRAWOZDANIE Z FUNKCJONOWANIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

Raz do roku do 30 stycznia Administrator przygotowuje w formie pisemnej sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych.

## 11 POSTANOWIENIA KOŃCOWE

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.

3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,

4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im upoważnień do przetwarzania danych osobowych.

6. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce bezpieczeństwa i innych zwanych z nią dokumentach.

7. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w RODO, ustawie i dokumentach wewnętrznych Organizacji, można wszcząć postępowanie dyscyplinarne.

8. Kara dyscyplinarna orzeczona wobec osoby winnej naruszenia zabezpieczeń systemu informatycznego i uchylającej się od powiadomienia administratora danych osobowych lub inspektora ochrony danych /jeśli został powołany/ nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

9. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO i ustawy.