Polityka Bezpieczeństwa Ochrony Danych Osobowych Mazowieckiej Izby Rzemiosła i Przedsiębiorczości w Warszawie

Warszawa 2018

Spis treści

Preambuła 3
Rozdział I Postanowienia ogólne 6
Rozdział II Dopuszczalność przetwarzania danych osobowych 8
Rozdział III Zbiory Danych osobowych 13
Rozdział IVZagrożenia i naruszenia ochrony danych osobowych 16
Rozdział V Zasady przetwarzania danych osobowych 18
Rozdział VI Postanowienia przejściowe i końcowe 20
Załączniki……22

Preambuła

Zważywszy, że:

- Z dniem 25 maja 2018 r., wchodzi w życie 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 osobowych),
- Mazowiecka Izba Rzemiosła i Przedsiębiorczości w Warszawie, w związku z prowadzoną działalnością statutową przetwarza dane osobowe zarówno pracowników, współpracowników jak i osób trzecich

Zarząd Mazowieckiej Izby Rzemiosła i Przedsiębiorczości w Warszawie, w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz zapewnienia zgodności przetwarzania danych osobowych z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz ustawy z dnia 10 maja 2018 r., o ochronie danych osobowych, przyjmuje niniejszą Politykę Bezpieczeństwa Ochrony Danych Osobowych Mazowieckiej Izby Rzemiosła i Przedsiębiorczości w Warszawie

§1
Definicje

Poniższym pojęciom nadaje się następujące brzmienie:

1. **Rozporządzenie** - 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 osobowych),
2. **Ustawa –** ustawa z dnia 10 maja 2018 r., o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000),
3. **Prezes Urzędu –** Prezes Urzędu Ochrony Danych Osobowych
4. **Polityka bezpieczeństwa –** niniejszy dokument określający cele, zakres i sposoby przetwarzania danych osobowych, dostosowujący odpowiednie środki techniczne i organizacyjne, z uwzględnieniem potencjalnego ryzyka i jest w szczególności przeznaczona dla pracowników Izby przetwarzających dane osobowe. opisujący procedury zapewnienia bezpieczeństwa danych osobowych w Izbie w tym w szczególności:

4.1 procedury określające sposób zabezpieczenia danych osobowych gromadzonych w postaci dokumentów sporządzanych w formie informatycznej oraz w formie innej niż informatyczna, w tym pisemnej,
4.2 organizacyjne i techniczne środki zabezpieczenia danych,
4.3 klauzule informacyjne uwzględniające prawa przysługujące osobom przekazującym dane osobowe Izbie lub podmiotom podległym,
4.4 regulamin wykorzystania systemów monitoringu wizyjnego **(Załącznik Nr 1)**
4.5 osób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.

5. **Administrator Danych Osobowych (ADO)** – Mazowiecka Izba Rzemiosła i Przedsiębiorczości w Warszawie, ul. Smocza 27, 01-048 Warszawa, dla której Sąd Rejonowy dla m. st. Warszawy XII Wydział Gospodarczy prowadzi akta rejestrowe KRS: 0000122864, tel. 22 838 32 11, fax 22 838 35 53, www.mirip.org.pl, e-mail: sekretariat@mirip.org.pl, zwany również dalej „Izbą" lub „Administratorem"
6. **Rejestr** - Rejestr zbiorów danych osobowych przetwarzanych przez Mazowiecką Izbę Rzemiosła i Przedsiębiorczości w Warszawie.
7. **Rejestr czynności przetwarzania danych osobowych –** rejestr działań Administratora i współadministratorów danych osobowych polegających na przetwarzaniu danych osobowych **(Załącznik Nr 2)**
8. **Instrukcja Zarządzania Systemem Informatycznym –** Zasady postępowania z systemem informatycznym Administratora w celu ochrony przetwarzanych danych osobowych **(Załącznik Nr 3)**
9. **Zabezpieczenia organizacyjne** - procedury określone w niniejszym Rozdziale II Polityki bezpieczeństwa oraz procedury określone w **Instrukcji zarządzania systemem informatycznym**,
10. **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej**.** Wśród danych osobowych wyróżniamy

10.1 **Dane wrażliwe** – dane osobowe, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym oraz dotyczące osób skazanych wyrokami sądów, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

10.2 **Dane genetyczne** - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

10.3 **Dane biometryczne** - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

10.4 **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

11. **Zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, czy dostępny jest w formie papierowej czy też elektronicznej.

12. **Strona trzecia -** osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
13. **Zgoda osoby, której dane dotyczą -** dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
14. **Osoba upoważniona** – osoba posiadająca upoważnienie wydane przez administratora danych osobowych lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w danej komórce organizacyjnej w zakresie wskazanym w upoważnieniu.
15. **Użytkownik systemu** – osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
16. **Odbiorca -** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
17. **Przetwarzanie -** operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, 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.
18. **Przetwarzający -** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
19. **Ograniczenie przetwarzania -** oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
20. **Profilowanie -** dowolna forma zautomatyzowanego przetwarzania danych osobowych, które 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**.**
21. **Pseudonimizacja -** przetwarzanie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
22. **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.

23. **Usuwanie danych** o**sobowych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
24. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
25. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez IODO lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
26. **Zasada „czystego biurka i białej kartki"** – zasady postępowania z dokumentami zawierającymi dane osobowe po zakończeniu pracy, stanowiące **Załącznik Nr 4**
27. **Urządzenie mobilne** – każde urządzenie elektroniczne za pomocą którego można przetwarzać dane osobowe, w szczególności laptopy, notebooki, tablety, telefony komórkowe

.

Rozdział I
Postanowienia ogólne

§2
Przetwarzanie danych osobowych

1. Mazowiecka Izba Rzemiosła i Przedsiębiorczości w Warszawie przetwarza dane osobowe w celu:
   1.1 Wykonywania obsługi biurowej i organizacyjnej organów statutowych Izby,
   1.2 Zrządzania danymi osobowymi pracowników etatowych Izby oraz osób fizycznych współpracujących z Izbą na innej podstawie prawnej niż umowa o pracę,
   1.3 Realizacji projektów z udziałem wsparcia finansowego ze środków Unii Europejskiej, zgodnie z zasadami określonymi odrębnymi przepisami odnoszącymi się do poszczególnych „źródeł wsparcia",
   1.4 Realizacji zadań związanych z prowadzeniem działalności oświatowej w ty, w szczególności w zakresie przeprowadzania egzaminów czeladniczych i mistrzowskich,
2. Zbiory danych osobowych, o których mowa w §2 ust 1 pkt. 1.1) – 1.4), gromadzone są w bazach danych w wersjach papierowych oraz w postaci zapisów elektronicznych z wykorzystaniem systemu informatycznego.

§3
Administrator Danych Osobowych

Administrator Danych Osobowych zapewnia:

1. Organizację bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami Rozporządzenia, Ustawy i innych właściwych przepisów,
2. Stosowanie środków technicznych i organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych zapewniających ochronę danych osobowych, a w szczególności:
   1.2.1. zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym,

1.2.2. zapobieganie przed zabraniam dokumentów przez osobę nieuprawnioną,
1.2.3. zapobieganie przetwarzaniu danych przez osoby nieupoważnione oraz utracie i uszkodzeniu danych.
1.2.4. Uwzględnianie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych.
1.2.5. Prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych.
1.2.6. Nadzór nad bezpieczeństwem danych osobowych, w tym kontrolę działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
1.2.7. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
1.2.8. Udzielanie pełnomocnictw do przetwarzania danych osobowych:
1.2.8.1 osobom wchodzącym w skład organów organizacji,
1.2.8.2 pracownikom,
1.2.8.3 współpracownikom,
1.2.8.4 wolontariuszom, praktykantom i stażystom,
1.2.8.5 pracownikom lub współpracownikom Izby w związku z realizacją projektów i zadań, w których Izba jest lub może być partnerem,
1.2.8.6 pracownikom lub współpracownikom instytucji, którym Izba powierzy na mocy pisemnej umowy – prowadzenie zadań z zakresu monitoringu i ewaluacji projektu/zadania, którego Izba jest realizatorem,
1.2.8.7 pracownikom Izby w związku z pozostałymi przypadkami przetwarzania danych osobowych w Izbie,
1.2.8.8 innym osobom gdy zajdzie taka uzasadniona potrzeba.

3. Udzielanie oraz odwoływanie pełnomocnictw dla Inspektora Ochrony Danych Osobowych oraz – jeśli występuje - dla Administratora Systemu Informatycznego.
4. Prowadzenie Ewidencji osób upoważnionych do przetwarzania danych,
5. Pełnomocnictwa oraz ich odwołanie ma formę pisemną i udzielane są na czas wykonywania przez osobę upoważnioną czynności na powierzonym stanowisku.
6. Wzór pełnomocnictwa do przetwarzania danych osobowych stanowi **Załącznik nr 5**, do Polityki bezpieczeństwa, natomiast wzór Ewidencji osób upoważnionych do przetwarzania danych **Załącznik nr 6** do Polityki bezpieczeństwa.

§4
Inspektor Ochrony Danych Osobowych

1. Inspektor Ochrony Danych Osobowych (IODO) jest powoływany przez Administratora. W przypadku powołania IODO, Administrator zawiadamia o tym fakcie Prezesa Urzędu w terminie 14 (czternastu) dni od jego wyznaczenia. Dane IODO wskazane w Ustawie udostępniane są również na stronie internetowej Administratora.
2. Funkcję IODO może pełnić pracownik Administratora lub podmiot zewnętrzny na podstawie umowy cywilnoprawnej,
3. IODO jest upoważniony do przetwarzania wszystkich zbiorów danych osobowych zewidencjonowanych w Rejestrze.
4. Do zadań IODO należy:

4.1 Współpraca z Administratorem przy realizacji zadań z zakresu ochrony danych osobowych, w tym nadzór nad bezpieczeństwem danych osobowych oraz kontrola działania komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

4.2 Zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

4.2.1 Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora,

4.2.2 Nadzorowanie opracowania i aktualizacji dokumentacji dotyczącej Polityki bezpieczeństwa danych osobowych u Administratora,

4.2.3 Zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

4.2.4 Prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez Administratora,

4.2.5 Kontrolę wykonywania operacji przetwarzania danych osobowych przez osoby upoważnione,

4.2.6 Zwracanie się do Administratora w przypadku istotnych wątpliwości wynikających ze stosowania przepisów ustawy o ochronie danych osobowych oraz przepisów wykonawczych,

4.2.7 Niezwłoczne poinformowanie Administratora o zaprzestaniu wykonywania czynności przetwarzania danych osobowych przez osobę upoważnioną.

5. Sprawowanie nadzoru nad przestrzeganiem zasad ochrony danych osobowych poprzez zapewnienie bezpieczeństwa danych osobowych w systemie informatycznym, w szczególności poprzez przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
6. Prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych,
7. Podejmowanie z własnej inicjatywy lub na wniosek Administratora działań zmierzających do ulepszenia ochrony danych osobowych w Izbie,
8. Prowadzenie ewidencji urządzeń mobilnych będących własnością Administratora na których są przetwarzane dane osobowe. Rejestr obejmuje co najmniej rodzaj urządzenia, jego markę i numer seryjny, dane osoby korzystającej i rodzaj przetwarzanych danych osobowych,

Rozdział II
Dopuszczalność przetwarzania danych osobowych

§5
Zasady ogólne

Dane osobowe muszą być:

1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,

2. Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
3. Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
4. Prawidłowe i w razie potrzeby uaktualniane,
5. Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, nie dłuższy niż jest to niezbędne do celów w których dane te są przetwarzane;
6. Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą , zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

§6
Warunki przetwarzania danych osobowych

Przetwarzanie Danych osobowych może odbywać się jedynie w poniższych warunkach:

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych, bądź osobę przez niego upoważnioną,
2. 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 Nr 7** do Polityki bezpieczeństwa,
3. Dane osobowe mogą być przetwarzane jedynie się na przystosowanych do tego stanowiskach pracy i tylko według zasad określonych w Polityce bezpieczeństwa,
4. W sytuacji naruszenia ochrony danych osobowych stosowana będzie określona w Polityce bezpieczeństwa procedura postępowania zmierzająca do usunięcia skutków naruszenia oraz ochrony praw osób zainteresowanych
5. Osoby przetwarzające dane osobowe w trakcie wykonywania powierzonych im zadań:
    5.1 zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie potrzeby przestrzegania bezpieczeństwa w trakcie pracy w systemie informatycznym Izby,
    5.2 zostały zobowiązane do zachowania ich w tajemnicy,
6. Przetwarzanie danych osobowych dokonywane jest w warunkach chroniących je przed dostępem osób nieupoważnionych.
7. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
8. Administrator prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych,
9. Wprowadzone zostały zasady „czystego biurka” i „białej kartki”.
10. Wprowadzone zostały zasady korzystania z poczty elektronicznej, stanowiące **Załącznik Nr 8** do Polityki bezpieczeństwa,

11. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła,
12. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób,
13. Nie udziela się informacji zawierających dane osobowe przez telefon, względnie udziela się je po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych.
14. Dostęp do pomieszczeń w których przetwarzane są dane osobowe jest możliwy tylko dla upoważnionych pracowników.

§7

Środki zabezpieczenia danych osobowych przechowywanych w postaci papierowej

1. Szafy i urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach,
2. 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,
3. Jednostkami zbiorów danych osobowych gromadzonych i przetwarzanych w wersji papierowej są:
   3.1 Segregatory zawierające teczki, w których gromadzone są oryginalne dokumenty w formie kart papierowych;
   3.2 Rejestry w postaci druku zwartego, introligowane w sposób uniemożliwiający usuwanie poszczególnych kart, z których każda jest oznaczona kolejnym numerem stanowiącym liczbę naturalną.
4. 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.
5. 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.
6. Zapasowe komplety kluczy do pomieszczeń przechowywane są w kasie pancernej Dyrektora Izby, ruch kluczy zapasowych podlega kontroli przez Dyrektora Izby. Każde pobranie i zdanie zapasowego klucza powinno być potwierdzone własnoręcznym podpisem pobierającego. Wzór rejestru pobrań kluczy zapasowych stanowi **Załącznik Nr. 9**
7. Wykaz pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych wraz z wykazem pracowników upoważnionych do odbierania kluczy stanowi **Załącznik nr 10** do Polityki bezpieczeństwa.

§8
Środki zabezpieczenia sieci komputerowej

1. Wewnętrzną sieć komputerowa Izby oraz poszczególne stanowiska pracy zabezpieczono przed dostępem osób nieuprawnionych oraz poprzez odseparowanie od sieci publicznej za pomocą urządzeń zabezpieczających,
2. Szczegółowe zasady postępowania z systemami informatycznymi Izby zostały określone w Instrukcji Zarządzania Systemem Informatycznym

§9
Prawa osób, których dane dotyczą

1. Osoba, której dane osobowe są przetwarzane:
   1.1 ma prawo do tego by, o ile nie dysponuje już tymi informacjami, w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie uzyskać wszelkie informacje dotyczące:
      1.1.1 tożsamości Administratora,
      1.1.2 danych kontaktowych IODO,
      1.1.3 celu przetwarzania danych osobowych,
      1.1.4 prawnie uzasadnionego celu przetwarzania danych osobowych, jeśli przetwarzanie jest niezbędne dl realizacji takiego celu,
      1.1.5 odbiorców danych osobowych lub kategorii odbiorców danych osobowych, jeśli tacy istnieją,
      1.1.6 informację o zamiarze przekazania danych osobowych do państwa trzeciego, jeśli ma to zastosowanie,
      1.1.7 okres przez który dane osobowe będą przechowywane, a jeśli nie jest możliwe – kryteria ustalania tego okresu,
      1.1.8 informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
      1.1.9 prawa do cofnięcia zgody na przetwarzanie danych w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem – o ile taka zgoda była wymagana,
      1.1.10 prawa wniesienia skargi do organu nadzorczego,
      1.1.11 tego, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do do ich podania i jakie są ewentualne konsekwencje niepodania danych,
      1.1.12 informacje o zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu,
   1.2 jeśli danych osobowych nie pozyskano od niej, ma prawo do otrzymania informacji dotyczących:
      1.2.1 tożsamości i danych kontaktowych Administratora, oraz gdy ma to zastosowanie i danych kontaktowych przedstawiciela,
      1.2.2 danych kontaktowych IODO,
      1.2.3 celu i podstawy prawnej przetwarzania danych osobowych,
      1.2.4 kategorii danych osobowych,

1.2.5 odbiorców danych osobowych lub kategorii odbiorców danych osobowych, jeśli tacy istnieją,
1.2.6 zamiaru przekazania danych do państwa trzeciego,
1.2.7 okresu przez który dane osobowe będą przechowywane, a jeśli nie jest możliwe – kryteria ustalania tego okresu,
1.2.8 prawnie uzasadnionych interesów realizowanych przez Administratora,
1.2.9 prawa żądania od Administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawa do wniesienia sprzeciwu wobec przetwarzania oraz prawa do przenoszenia danych,
1.2.10 prawa do cofnięcia zgody na przetwarzanie danych w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem – o ile taka zgoda była wymagana,
1.2.11 prawa wniesienia skargi do organu nadzorczego,
1.2.12 źródle pochodzenia danych osobowych oraz informacje czy pochodzą one z publicznego źródła,
1.2.13 informacje o zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu,

1.3 ma prawo do uzyskania od Administratora potwierdzenia czy przetwarzane są dane osobowe jej dotyczące a jeśli ma to miejsce ma prawo do uzyskania dostępu do nich oraz następujących informacji:
1.3.1 cel przetwarzania,
1.3.2 kategorie odnośnych danych osobowych,
1.3.3 informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
1.3.4 planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe kryteria ustalenia tego okresu,
1.3.5 prawo żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawa do wniesienia sprzeciwu wobec przetwarzania,
1.3.6 prawo do wniesienia skargi do organu nadzorczego,
1.3.7 dotyczących źródeł danych osobowych – jeśli nie zostały one zebrane od osoby, której dotyczą,
1.3.8 informacje o zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu,

2. Osoba, której dane są przetwarzane ma prawo do żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba której prawa dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia,
3. Osoba, której dane są przetwarzane ma prawo żądania od Administratora niezwłocznego usunięcia danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć te dane, jeśli zachodzi jedna z następujących okoliczności:
3.1 dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
3.2 osoba, której dane dotyczą cofnęła zgodę,

3.3 osoba, której dane dotyczą zgłosiła sprzeciw w trybie art. 21 Rozporządzenia i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
3.4 dane osobowe były przetwarzane niezgodnie z prawem,
3.5 dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator,
3.6 dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego o których mowa w art. 8 ust 1 Rozporządzenia,

4. Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania jeśli:
   4.1 kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzenie prawidłowości tych danych,
   4.2 przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu tych danych żądając w zamian ograniczenia ich przetwarzania,
   4.3 Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie której dotyczą do ustalenia, dochodzenia lub obrony roszczeń,
   4.4 Wniosła sprzeciw na podstawie art. 21 Rozporządzenia,
5. Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi bez przeszkód ze strony administratora, któremu te dane dostarczono jeżeli przetwarzanie odbywa się na podstawie zgody lub w sposób zautomatyzowany,
6. Osoba której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania jej danych osobowych opartego na art. 6 ust 1 lit e) i f) Rozporządzenia w tym profilowaniu na podstawie tych przepisów. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów,
7. Osoba, której dane dotyczą, z zastrzeżeniem wyjątków przewidzianych w art. 22 ust 2 Rozporządzenia ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Rozdział III
Zbiory Danych osobowych

§10
Wykaz zbiorów danych osobowych

1. Administrator przetwarza Dane osobowe w następujących zbiorach:
   1.1 Ewidencja osób upoważnionych do przetwarzania danych osobowych w następujących polach: imię i nazwisko, telefon. Dane przetwarzane są w formie elektronicznej i papierowej.
   1.2 Akta osobowe pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.

1.3 Zbiory informacji o pracownikach, oświadczenia na potrzeby Zakładowego Funduszu Świadczeń Socjalnych, w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie papierowej.
1.4 Zbiory informacji o pracownikach na potrzeby Pracowniczej Kasy Zapomogowo Pożyczkowej, w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email, wysokość pobranych pożyczek, terminy spłat, wysokość zadłużenia, potrącenia z wynagrodzenia z tytułu spłaty udzielonej pożyczki. Dane przetwarzane są w formie papierowej.
1.5 Ewidencja zwolnień lekarskich w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.6 Skierowania na badania okresowe w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.7 Ewidencja urlopów, czasu pracy i wyjść w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.8 Rejestr delegacji służbowych w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie i papierowej.
1.9 Listy płac pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.10 Deklaracje ubezpieczeniowe pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.11 Deklaracje i kartoteki ZUS pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.12 Deklaracje podatkowe pracowników, w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.13 Rejestr wypadków w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie papierowej.
1.14 Rejestr umów najmu z najemcami w następujących polach: podmiot, imię i nazwisko osób reprezentujących, adres siedziby, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.15 Rejestr umów z innymi podmiotami zewnętrznymi /kontrahentami/ w następujących polach: podmiot, NIP, imię i nazwisko osób reprezentujących, adres siedziby, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
1.16 Rejestr czynności przetwarzania danych osobowych. Dane przetwarzane są w formie elektronicznej.
1.17 Rejestr członków Izby w następujących polach: nazwa organizacji, adres, telefon kontaktowy, adres email. Dane przetwarzane są w formie papierowej i elektronicznej.

1.18 Rejestr Delegatów na Kongres Mazowieckiej Izby Rzemiosła i Przedsiębiorczości w następujących polach: nazwa organizacji, imię i nazwisko delegata, data urodzenia, adres zamieszkania, adres zakładu pracy, telefon, wykształcenie. Dane przetwarzane są w wersji papierowej i elektronicznej.

1.19 Pocztowa książka nadawcza w następujących polach: adresat instytucja, imię i nazwisko, adres miejsca doręczenia. Dane przetwarzane są w wersji papierowej.

1.20 Rejestr kandydatów do uzyskania tytułu czeladnika oraz mistrza w następujących polach: imię nazwisko, numer PESEL, numer NIP, wykształcenie, doświadczenie zawodowe. Rejestr prowadzony jest w formie papierowej i elektronicznej,

1.21 Rejestr kandydatów do zatrudnienia w Izbie obejmujący imię nazwisko, datę urodzenia, doświadczenie zawodowe, kwalifikacje zawodowe w tym znajomość języków, wykształcenie. Dane przetwarzane są w formie papierowej i elektronicznej,

1.22 Rejestr wniosków o wydanie duplikatu świadectwa (bez rejestru) w następujących polach: imię i nazwisko, data i miejsce urodzenia, PESEL, adres zamieszkania, dane świadectwa /nr księgi wieczystej, data wydania/. Dane przetwarzane są w wersji elektronicznej i papierowej.

1.23 Rejestr odznaczeń w następujących polach: organizacja, imię i nazwisko, przyznane odznaczenia, data przyznania), imiona rodziców, data i miejsce urodzenia, miejsce zamieszkania, wykonywane rzemiosło lub zawód, miejsce zatrudnienia, okresy członkostwa w organizacjach, pełnione funkcje samorządowe, przyznane odznaczenia. Dane przetwarzane są w wersji papierowej i elektronicznej.

1.24 Rejestr byłych i obecnych pracowników, osób zatrudnionych na umowy cywilnoprawne i innych osób współpracujących w następujących polach: imię i nazwisko, PESEL, NIP, data urodzenia, miejsce urodzenia, adres zameldowania, adres zamieszkania, adres do korespondencji, telefon, adres e-mail, nr rachunku bankowego. Dane przetwarzane są w formie papierowej i elektronicznej.

1.25 Rejestr byłych i obecnych pracowników, osób zatrudnionych na umowy cywilnoprawne i innych osób współpracujących w następujących polach: imię i nazwisko, PESEL, seria i nr dowodu osobistego, data urodzenia, miejsce urodzenia, adres zameldowania, adres zamieszkania, adres do korespondencji, telefon, adres e-mail. Dane przetwarzane są w formie papierowej i elektronicznej.

1.26 Archiwum - obejmujące dokumentację archiwalną zlikwidowanych organizacji rzemieślniczych, akta osobowe pracowników, dokumentacja kadrowo - płacowa (wersja papierowa), zbiory danych osobowych uczestników projektów realizowanych przez organizację współfinansowanych ze środków Unii Europejskiej.

Rozdział IV
Zagrożenia i naruszenia ochrony danych osobowych

§11
Zagrożenia naruszeń danych osobowych

Zagrożeniami naruszenia bezpieczeństwa danych osobowych są:

1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu – ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2. Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3. Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych – zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy.

§12
Naruszenie ochrony danych osobowych

Naruszeniem ochrony danych osobowych są:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana,
2. napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
3. niekorzystne parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
4. awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub sabotaż;
5. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
6. pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
7. naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
8. stwierdzona próba modyfikacji lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
9. niedopuszczalna manipulacja danymi osobowymi w systemie;
10. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą,
11. procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
12. nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie lub sieci komputerowej wskazujące na przełamanie lub zaniechanie ochrony danych osobowych np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;
13. istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki” itp.;

14. podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
15. rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).
16. nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, nośnikach elektronicznych w formie niezabezpieczonej itp.

§13
Zasady postępowania w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia:
   1.1 naruszenia zabezpieczeń systemu informatycznego,
   1.2 naruszenia technicznego stanu urządzeń,
   1.3 naruszenia zawartości zbioru danych osobowych,
   1.4 ujawnienia metody pracy lub sposobu działania programu,
   1.5 pogorszenia jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   1.6 innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

   Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie IODO.
2. W razie niemożliwości zawiadomienia IODO lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia danych osobowych IODO lub upoważnionej przez niego osoby, należy:

3.1 Niezwłocznie – o ile istnieje taka możliwość – podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia oraz ustalić przyczyny lub sprawców naruszenia danych osobowych.

3.2 Udokumentować wstępnie zaistniałe naruszenie,

3.3 Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IODO lub osoby przez niego upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia danych osobowych, IODO lub osoba przez niego upoważniona:

4.1 Zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji.

4.2 Żąda zdania dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4.3 Powiadamia Administratora o zaistniałym naruszeniu lub ujawnieniu danych osobowych,
4.4 Jeżeli zachodzi taka potrzeba nawiązuje bezpośredni kontakt z zewnętrznymi specjalistami powiadamiając o tym jednocześnie Administratora
5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, IODO zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
6. IODO dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport ze zdarzenia
7. Raport, o którym mowa w ust. 6, IODO niezwłocznie przekazuje Administratorowi. Wzór raportu stanowi **Załącznik nr 11** do „Polityki bezpieczeństwa".
8. Po dokonaniu czynności sprawdzających oraz po przeprowadzeniu analizy naruszenia danych osobowych, sporządza się protokół stanowiący podstawę do wprowadzenia zabezpieczeń technicznych i organizacyjnych mających zapobiec podobnym naruszeniom w przyszłości.

Rozdział V
Zasady przetwarzania danych osobowych

§14
Zasady ogólne

1. Osoba upoważniona do przetwarzania danych zobowiązana jest do:
   1.1 Zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych.
   1.2 Zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą.
   1.3 Stosowania określonych przez Administratora procedur i środków przetwarzania oraz zabezpieczania danych osobowych.
   1.4 Podporządkowania się zgodnym z prawem poleceniom IODO i Administratora w zakresie ochrony danych osobowych,
   1.5 Zachowania danych osobowych w tajemnicy.
   1.6 Przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, a w szczególności:
      1.6.1 zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem,
      1.6.2 zabezpieczenia danych osobowych przed ich zmianą,
      1.6.3 zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
      1.6.4 zamykania i zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,
      1.6.5 dopilnowania, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej,

1.6.6 dopilnowania, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie,

1.6.7 przetwarzania, udostępniania danych osobowych zgodnie z celem, dla którego zostały zebrane.

2. Każda osoba upoważniona do przetwarzanie danych osobowych powinna odbyć szkolenie z zakresu ochrony danych osobowych. Szkolenie z zakresu ochrony danych osobowych organizuje IODO.
3. Rejestr zbiorów danych osobowych przetwarzanych w organizacji prowadzony jest w formie papierowej i/lub elektronicznej przez IODO.

§ 15

Zasady korzystania z urządzeń mobilnych, na których są przetwarzane dane osobowe

1. W przypadkach uzasadnionych potrzebą Administratora możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem przy użyciu urządzeń mobilnych, jednak wymaga to każdorazowego zawiadomienia IODO,
2. Przetwarzanie danych osobowych, o którym jest mowa w ust 1 możliwe jest jedynie na urządzeniach mobilnych będących własnością Administratora. W przypadku urządzeń mobilnych będących własnością osób trzecich konieczna jest uzyskanie zgody IODO. O każdym takim przypadku IODO powiadamia Administratora,
3. Osoba korzystająca z urządzenia mobilnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, w szczególności do:
    3.1 transportu urządzenia mobilnego w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
    3.2 korzystania z urządzenia mobilnego w sposób minimalizujący ryzyko uzyskania dostępu do przetwarzanych danych przez osoby nieupoważnione,
    3.3 zabezpieczania urządzenia mobilnego hasłem;
    3.4 blokowania dostępu do urządzenia mobilnego w przypadku, gdy nie jest on wykorzystywany przez pracownika;
    3.5 kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych;
    3.6 bieżącej aktualizacji baz wirusowych programu antywirusowego zainstalowanego na urządzeniu mobilnym,
    3.7 utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł;
    3.8 wykorzystywania haseł odpowiedniej jakości (co najmniej na poziomie „średnie") zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe;
    3.9 zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.
    3.10 Natychmiastowego zawiadomienia IODO albo Administratora lub bezpośredniego przełożonego o kradzieży urządzenia mobilnego lub o innych zdarzeniach mogących stanowić naruszenie lub zagrożenia ochrony danych osobowych,

4. IODO zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:
    4.1 Dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,
    4.2 Zabezpieczono dane osobowe przetwarzane na komputerach przenośnych poprzez zastosowanie oprogramowania szyfrującego te dane. Dostęp do danych jest możliwy wyłącznie po podaniu tego hasła,
    4.3 Dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerach przenośnych.
    4.4 Przeprowadzono aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

§16
Przetwarzanie danych osobowych powierzonych przez Izbę innym podmiotom

1. Administrator w uzasadnionym przypadku może powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu, na podstawie umowy zawartej w formie pisemnej pod rygorem nieważności. Wzór umowy powierzenia stanowi **Załącznik nr 12** do Polityki bezpieczeństwa.
2. Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi **Załącznik nr 13**
3. Możliwe jest przetwarzanie w Izbie danych osobowych powierzonych Izbie przez inny podmiot (Zleceniodawcę). W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie umowy między Izbą a Zleceniodawcą zawartej w formie pisemnej pod rygorem nieważności.
4. Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością Izby, chyba, że umowa określi inne, surowsze zasady ochrony danych osobowych. W szczególności może dotyczyć to nadawania uprawnień do przetwarzania danych osobowych.
5. Dostęp do powierzonych danych osobowych z sieci zewnętrznej (np. siedziby Zleceniodawcy) musi odbywać się z zachowaniem odpowiednich zabezpieczeń. W przypadku danych elektronicznych, dostęp do nich musi być chroniony identyfikatorem oraz hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.
6. W przypadku przetwarzania danych związanych z obsługą projektów UE, administratorem danych jest również instytucja pośrednicząca, zarządzająca lub wdrażająca dany program unijny. Dane przetwarzane są na podstawie odrębnych umów.

Rozdział VI
Postanowienia przejściowe i końcowe

§17
Wejście Polityki bezpieczeństwa w życie

1. Polityka bezpieczeństwa wchodzi w życie z dniem 25 maja 2018 r.
2. Polityka bezpieczeństwa będzie umieszczona na stronie internetowej Administratora oraz wyłożona do wglądu dla pracowników w komórce odpowiedzialnej za prowadzenie spraw kadrowych,

§18
Przepisy przejściowe

Z dniem wejścia w życie Polityki Bezpieczeństwa:

1. tracą moc wszelkie wewnętrzne akty prawne Administratora normujące kwestie uregulowane w Polityce bezpieczeństwa, w szczególności dotyczące przetwarzania i ochrony danych osobowych,
2. Osoby pełniące funkcję Administratora Bezpieczeństwa Informacji staje się IODO i pełni swoją funkcję do dnia 1 września 2018 r., chyba że przed tą datą Administrator zawiadomi Prezesa Urzędu o wyznaczeniu innej osoby w sposób wskazany w Ustawie,

§19
Wdrożenie Polityki bezpieczeństwa

1. Wdrożenie Polityki bezpieczeństwa odbywa się poprzez przeszkolenie osób wchodzących w skład organów organizacji, pracowników, współpracowników, praktykantów i stażystów organizacji z zaznajomienie użytkownika z przepisami Rozporządzenia, treścią Polityki bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u Administratora danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada IODO.
3. 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. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im upoważnień do przetwarzania danych osobowych.
4. Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, zobowiązany jest prowadzić IODO. Wzór ewidencji stanowi **Załącznik nr 14** do „Polityki bezpieczeństwa”.
5. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce bezpieczeństwa,
6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w Rozporządzeniu, innych aktach prawnych i Polityce bezpieczeństwa można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna orzeczona wobec osoby winnej naruszenia zabezpieczeń systemu informatycznego i uchylającej się od powiadomienia Administratora lub IODO nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

8. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
9. W sprawach nieuregulowanych w Polityce bezpieczeństwa mają zastosowanie przepisy Rozporządzenia oraz Ustawy
10. Załączniki do Polityki Bezpieczeństwa stanowią jej integralną część. Potwierdzenie zapoznania się z Polityka Bezpieczeństwa oznacza potwierdzenie zapoznania się z załącznikami.

Wykaz załączników:

1. Załącznik Nr 1 Regulamin monitoringu wizyjnego,
2. Załącznik Nr 2Rejestr czynności przetwarzania danych osobowych,
3. Załącznik Nr 3 Instrukcja Zarządzania Systemem Informatycznym,
4. Załącznik Nr 4 Zasada pustego biurka i czystej kartki,
5. Załącznik Nr 5 Pełnomocnictwo do przetwarzania danych osobowych,
6. Załącznik Nr 6 Ewidencja osób upoważnionych do przetwarzania danych osobowych,
7. Załącznik Nr 7 Oświadczenie pracownika,
8. Załącznik Nr 8 Zasady korzystania z poczty elektronicznej,
9. Załącznik Nr 9 Ewidencja pobrania kluczy zapasowych,
10. Załącznik Nr 10 Wykaz budynków i pomieszczeń,
11. Załącznik Nr 11 Raport naruszenia danych osobowych,
12. Załącznik Nr 12 Umowa o powierzenie przetwarzania danych osobowych,
13. Załącznik Nr 13 Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych,
14. Załącznik Nr 14 Ewidencja osób przeszkolonych