POLITYKA OCHRONY DANYCH OSOBOWYCH IZBY GOSPODARCZEJ HANDLOWCÓW, PRZETWÓRCÓW ZBÓŻ I PRODUCENTÓW PASZ

Zatwierdzam:

Monika Piątkowska

Prezydent

WSTĘP

Niniejszy dokument określa zasady przetwarzania i ochrony danych osobowych, jakie powinny być przestrzegane i stosowane w Izbie Gospodarczej Handlowców, Przetwórców Zbóż i Producentów Pasz („**Izba**") przez pracowników, osoby pełniące funkcje w organach Izby i współpracowników, którzy przetwarzają dane osobowe („**Polityka Ochrony Danych Osobowych**").

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony przetwarzanych przez Izbę danych osobowych rozumianej jako ochrona danych przed ich utratą, uszkodzeniem lub zniszczeniem oraz uzyskaniem do nich dostępu przez osoby nieupoważnione, zmianą, usunięciem lub zabraniem przez osobę nieuprawnioną oraz przed przetwarzaniem w sposób naruszający 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.

1.1 Definicje

ADO (Administrator Danych Osobowych) – Izba; podmiot, który ustala cele i sposoby przetwarzania danych Osobowych.

Bezpieczeństwo Systemu informatycznego - wdrożenie przez Administratora Danych Osobowych lub osobę przez niego upoważnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz Ochrony Danych Osobowych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

Dane Osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer PESEL, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Osoba Upoważniona – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych (lub osobę upoważnioną przez niego) i dopuszczona jako użytkownik do Przetwarzania Danych Osobowych w zakresie wskazanym w upoważnieniu.

Przetwarzanie Danych Osobowych – operacje lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki 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.

Rozporządzenie – Rozporządzenia 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 (opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1).

Stacja Robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający Osobie Upoważnionej dostęp do Danych Osobowych znajdujących się w systemie.

System Informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur i narzędzi programowych zastosowanych w celu Przetwarzania Danych Osobowych.

UODO – Urząd Ochrony Danych Osobowych.

Ustawa – polska ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych.

Użytkownik Systemu - osoba posiadająca uprawnienia do Przetwarzania Danych Osobowych w Systemie informatycznym.

1.2 Informacje ogólne

Polityka Ochrony Danych Osobowych została opracowana w oparciu o wytyczne zawarte w Rozporządzeniu oraz w Ustawie.

1.3 Zakres zastosowania

Politykę Ochrony Danych Osobowych stosuje się do Danych Osobowych przetwarzanych w Systemie Informatycznym, zapisanych na zewnętrznych nośnikach informacji, w tym dokumentów papierowych, oraz informacji dotyczących bezpieczeństwa Przetwarzania Danych Osobowych.

Polityka Danych Osobowych obowiązuje wszystkich pracowników Izby oraz inne osoby mające dostęp do Danych Osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło. Administrator Danych Osobowych zapewnia stosowanie zasad wynikających z niniejszej Polityki Ochrony Danych Osobowych przez podmioty przetwarzające Dane Osobowe na zlecenie Administratora.

1.4 Bezpieczeństwo Przetwarzania Danych Osobowych

Przez bezpieczeństwo Przetwarzania Danych Osobowych rozumie się zapewnienie:

a) zgodności z prawem, rzetelności i przejrzystości Przetwarzania Danych Osobowych;
b) ograniczenia celu – że Dane Osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są przetwarzane dalej w sposób niezgodny z tymi celami;
c) minimalizacji danych – że Dane Osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
d) prawidłowości – że Dane Osobowe są zgodne ze stanem faktycznym i w razie potrzeby uaktualniane;
e) ograniczenia przechowywania – że Dane Osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których Dane Osobowe są przetwarzane;
f) integralności i poufności — że Dane Osobowe są 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 oraz organizacyjnych;
g) rozliczalności — że ADO jest odpowiedzialny za przestrzeganie powyższych zasad i jest w stanie wykazać ich przestrzeganie.

1.5 Kategorie Danych Osobowych przetwarzanych w Izbie

Izba przetwarza następujące kategorie Danych Osobowych:

Lp.	Kategoria Danych Osobowych	Zakres Danych Osobowych	Okres przetwarzania	Uwagi
1.	Dane pracowników i współpracowników	Dane związane z zatrudnieniem, w tym dane zawarte w aktach osobowych oraz wizerunek pracownika	Przez okres zatrudnienia (obowiązywania umowy) oraz po ustaniu zatrudnienia, przez okres wymagany przepisami prawa, w tym dotyczącymi przechowywania akt osobowych	a) Dane Osobowe są przetwarzane wyłącznie w związku z zatrudnieniem; b) Dane Osobowe mogą być udostępniane podmiotom świadczącym na rzecz Izby usługi związane z zatrudnieniem i przywilejami pracowników oraz współpracowników, w tym

				w zakresie ubezpieczenia medycznego; c) Dane Osobowe, w postaci wizerunku, mogą być także przetwarzane do celów promocyjnych i informacyjnych Izby wyłącznie za dobrowolną zgodą pracownika lub współpracownika
2.	Dane Osobowe byłych pracowników i współpracowników	Dane związane z zatrudnieniem, w tym dane zawarte w aktach Osobowych	Po ustaniu zatrudnienia, przez okres wymagany przepisami prawa, w tym dotyczącymi przechowywania akt osobowych	Jak wyżej w pkt 1
3.	Dane Osobowe kandydatów do pracy	Dane podawane zgodnie z Kodeksem pracy lub – w przypadku zatrudnienia na innej podstawie: a) imię i nazwisko; b) datę urodzenia; c) numer telefonu; d) adres e-mail; e) adres do korespondencji	Przez okres prowadzenia danego postępowania rekrutacyjnego oraz przez dalszy okres – jeżeli kandydat wyraził zgodę na dalsze przetwarzanie jego Danych Osobowych	Dane są przetwarzane w związku z prowadzeniem postępowania rekrutacyjnego oraz, za zgodą kandydata, także w związku z innymi rekrutacjami
4.	Dane Osobowe kontrahentów i oraz Dane Osobowe osób reprezentujących kontrahentów– przedsiębiorców	Dane kontaktowe, w tym: a) imię i nazwisko; b) numer telefonu; c) adres e-mail	Przez okres obowiązywania umowy o współpracę oraz okres niezbędny do dokonania rozliczeń pomiędzy stronami po rozwiązaniu lub wygaśnięciu umowy	Dane są przetwarzane wyłącznie w związku z wykonaniem umowy lub w związku z czynnościami mającymi na celu zawarcie umowy
5.	Dane Osobowe członków Rady Izby i innych organów Izby	Dane podawane w celu wyboru do organów Izby : a) imię i nazwisko; b) data urodzenia; c) numer PESEL	Przez okres pełnienia funkcji członka Rady Izby lub funkcji w innym organie Izby	Dane są przetwarzane w związku z pełnieniem funkcji członka Rady Izby lub pełnieniem funkcji w innym organie Izby
6.	Dane osobowe osób reprezentujących (członków Izby) w Izbie	Dane kontaktowe: a) imię i nazwisko; b) numer telefonu; c) adres e-mail, d) stanowisko	Przez okres członkostwa w Izbie	Dane są przetwarzane w związku z członkostwem podmiotu w Izbie

1.6 Przetwarzanie szczególnych kategorii Danych Osobowych

1. ADO nie przetwarza szczególnych kategorii Danych Osobowych, z wyjątkiem sytuacji przewidzianych w art. 9 ust. 2 Rozporządzenia.
2. Przez szczególne kategorie Danych Osobowych rozumie się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej (np. wizerunek twarzy lub dane daktyloskopijne), dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

2 OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

Osobą odpowiedzialną za Przetwarzanie Danych osobowych oraz za ich ochronę zgodnie z postanowieniami Rozporządzenia, Ustawy oraz Polityki Ochrony Danych Osobowych jest ADO.

Bez względu na powyższe, wszystkie osoby przetwarzające Dane Osobowe w imieniu ADO, w tym Osoby Upoważnione, są zobowiązane do zapewnienia bezpieczeństwa Przetwarzania Danych Osobowych.

2.1 Administrator Danych Osobowych

ADO jest Izba Gospodarcza Handlowców, Przetwórców Zbóż i Producentów Pasz z siedzibą w Warszawie przy ul. Wspólnej 56, 00-684 Warszawa. Obowiązki **ADO** wykonuje Sekretarz Generalny Izby.

2.1.1 Obowiązki ADO

1. Zapewnienie prawidłowości przetwarzania oraz skutecznej ochrony Danych Osobowych zgodnie z zasadami wynikającymi z Rozporządzenia.
2. Wyznaczenie i podział zadań i obowiązków związanych z ochroną Danych Osobowych.
3. Wprowadzenie procedur oraz środków technicznych i organizacyjnych zapewniających prawidłowe Przetwarzanie Danych Osobowych oraz możliwość wykazania prawidłowości Przetwarzania Danych Osobowych.
4. Zapewnienie aktualizacji środków bezpieczeństwa Przetwarzania Danych Osobowych.
5. Zapewnienie okresowych przeglądów skuteczności Polityki Ochrony Danych Osobowych.
6. Prowadzenie rejestru czynności Przetwarzania Danych osobowych zgodnie z **Załącznikiem nr 1** do niniejszej Polityki Ochrony Danych Osobowych.
7. Pełnienie funkcji punktu kontaktowego dla UODO w kwestiach związanych z Przetwarzaniem Danych Osobowych.
8. Nadawanie upoważnień do Przetwarzania Danych Osobowych i prowadzenie ewidencji Osób upoważnionych do Przetwarzania Danych Osobowych.
9. Prowadzenie regularnych szkoleń z zakresu Ochrony Danych Osobowych.

2.2 Inspektor Danych Osobowych

Mając na względzie fakt, że główna działalność ADO nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; a także ze względu na fakt, że główna działalność ADO nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 Rozporządzenia w Spółce nie został wyznaczony Inspektor Danych Osobowych.

2.3 Osoby Upoważnione do Przetwarzania Danych Osobowych

Osoba Upoważniona powinna wykazywać znajomość zasad ochrony Danych Osobowych i powinna stosować w możliwie najszerszym zakresie wszelkie dostępne środki tej ochrony, co w szczególności dotyczy uniemożliwienia osobom nieuprawnionym dostępu do jej Stacji Roboczej i Przetwarzanych Danych Osobowych. Do obowiązków Osoby Upoważnionej należy również:

a) przetwarzanie Danych Osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami w Izbie;
b) zachowanie w tajemnicy Danych Osobowych oraz informacji o sposobach ich zabezpieczenia;
c) niezwłoczne informowanie ADO o wszelkich podejrzeniach incydentów związanych z naruszeniem zasad Przetwarzania Danych Osobowych lub zauważonych incydentach oraz słabościach w systemie ochrony Danych Osobowych, w szczególności Systemu Informatycznego.

3 ANALIZA RYZYKA PRZETWARZANIA DANYCH OSOBOWYCH

1. ADO przeprowadził analizę ryzyka Przetwarzania Danych Osobowych, zgodnie z **Załącznikiem nr 2** do niniejszej Polityki Ochrony Danych Osobowych, biorąc pod uwagę:
   a) mały zakres przetwarzania danych osobowych, w tym nieprzetwarzanie danych szczególnych, zgodnie z pkt 1.5 i 1.6 niniejszej Polityki Ochrony Danych Osobowych;
   b) brak przesłanek wskazanych w art. 35 ust. 3 Rozporządzenia;
   c) małą skalę Przetwarzania danych osobowych;
   d) zastosowane środki zabezpieczeń, w szczególności wskazane w pkt 6, 7 i 8 niniejszej Polityki Ochrony Danych Osobowych;
   e) małą liczbę osób upoważnionych do Przetwarzania Danych osobowych.
2. Po przeprowadzonej analizie ryzyka ADO uznał, że Przetwarzanie Danych Osobowych w Spółce ze względu na swój charakter, zakres, kontekst i cele nie może powodować z dużym prawdopodobieństwem wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, i w związku z tym odstąpił od przeprowadzenia oceny skutków dla ochrony danych zgodnie z art. 35 Rozporządzenia.

4 REJESTR CZYNNOŚCI PRZETWARZANIA

ADO prowadzi rejestr czynności przetwarzania danych osobowych. Rejestr prowadzony jest w formie pisemnej i stanowi **Załącznik nr 1** do niniejszej Polityki Ochrony Danych Osobowych. Rejestr może być także prowadzony w formie elektronicznej w formacie pliku excel.

5 PRAWA OSÓB, KTÓRYCH DANE OSOBOWE DOTYCZĄ

5.1 Podstawowe zasady

1. Osoba, której Dane Osobowe są przetwarzane, jest uprawniona do:
   a) otrzymania informacji o danych ADO, zasadach przetwarzania danych oraz przysługujących jej uprawnieniach, na zasadach określonych w pkt 5.2 poniżej;
   b) uzyskania potwierdzenia, czy przetwarzane są dane jej dotyczące, a jeżeli ma to miejsce – uzyskania dostępu oraz otrzymania informacji, o których mowa w pkt 5.3. poniżej (prawo dostępu);
   c) żądania niezwłocznego sprostowania dotyczących jej Danych Osobowych, które są nieprawidłowe oraz (z uwzględnieniem celów przetwarzania) żądania uzupełniania niekompletnych danych Osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia;
   d) żądania niezwłocznego usunięcia dotyczących jej Danych Osobowych (prawo do bycia zapomnianym);
   e) żądania ograniczenia przetwarzania Danych Osobowych;
   f) przenoszenia Danych Osobowych;
   g) wniesienia sprzeciwu wobec przetwarzania dotyczących jej Danych Osobowych.
2. ADO nie podejmuje decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu Danych Osobowych, w tym profilowaniu.
3. Informacje, o których mowa w ust. 1 pkt b) oraz działania, o których mowa w ust. 1 pkt c)-g), podejmowane są na wniosek zainteresowanego. Wnioski powinny być kierowane na adres: Izba Gospodarcza Handlowców, Przetwórców Zbóż i Producentów Pasz z siedzibą w Warszawie przy ul. Wspólnej 56, 00-684 Warszawa lub na adres e-mail: grain@izbazp.pl .
4. Rozpatrywaniem wniosków, o których mowa powyżej, zajmuje się Biuro Izby.
5. Jeżeli wniosek jest niepełny lub niejasny, w szczególności co do zakresu żądanych informacji, osoba rozpatrująca wniosek może zwrócić się do wnioskodawcy z prośbą o doprecyzowanie żądania.
6. Informacji o działaniach podjętych w związku z wnioskami, o których mowa w ust. 1 pkt b)-f) udziela się pisemnie (chyba że wnioskodawca wskaże inną formę) w terminie miesiąca od otrzymania wniosku.

7. Termin, o którym mowa w ust. 7, może być przedłużony o dwa miesiące ze względu na skomplikowany charakter żądania lub liczbę żądań. Wnioskodawca musi zostać poinformowany o przedłużeniu terminu oraz jego przyczynach.
8. Działania oraz udzielanie informacji, o których mowa w niniejszym artykule, nie wymagają wnoszenia przez wnioskodawcę żadnych opłat. Jeżeli żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, ADO może podjąć decyzję o:
   a) pobraniu opłaty w stosownej wysokości; lub
   b) odmowie podjęcia działań.
9. Osoba rozpatrująca wniosek ma prawo do weryfikacji tożsamości wnioskodawcy, o ile zachodzą co do tego wątpliwości. W tym celu może poprosić o okazanie dowodu osobistego lub innego dokumentu potwierdzającego tożsamość wnioskodawcy.
10. W terminie 14 dni ADO informuje o sprostowaniu lub usunięciu danych Osobowych lub ograniczeniu ich przetwarzania zgodnie z wnioskiem zainteresowanego, każdego odbiorcę, któremu ujawniono dane Osobowe, chyba że będzie to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

5.2 Informacja udzielana osobie, której dane dotyczą

1. Osoba, której dane dotyczą, otrzymuje od ADO następujące informacje:
   a) dane Izby jako administratora;
   b) o celu oraz podstawie prawnej Przetwarzania Danych Osobowych;
   c) o odbiorcy Danych Osobowych;
   d) o okresie, przez który Dane Osobowe będą przechowywane lub kryteriach ustalenia tego okresu;
   e) o prawie dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie wniesienia sprzeciwu wobec ich przetwarzania;
   f) o prawie do cofnięcia zgody w dowolnym momencie (jeżeli przetwarzanie danych odbywa się na podstawie zgody);
   g) o prawie wniesienia skargi do organu nadzorczego;
   h) informację, czy podanie danych jest wymogiem ustawowym czy umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
2. Informacje, o których mowa w ust. 1, są przekazywane przed rozpoczęciem Przetwarzania Danych Osobowych poprzez e-mail.
3. Informacji, o których mowa w ust. 1, nie podaje się, jeżeli osoba, której dane dotyczą, dysponuje już tymi danymi.

5.3 Prawo dostępu przysługujące osobie, której dane dotyczą

1. Osoba, której dane dotyczą, może uzyskać od ADO potwierdzenie, czy jej Dane Osobowe są przetwarzane, a jeżeli tak – że jest uprawniona do uzyskania dostępu do nich oraz uzyskania informacji o:
   a) celach przetwarzania;
   b) kategoriach przetwarzanych danych;
   c) odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione;
   d) planowanym okresie przechowywania danych Osobowych, a gdy nie jest to możliwe – o kryteriach ustalania tego okresu;
   e) przysługujących jej prawach;
   f) źródle danych, jeżeli nie zostały zebrane bezpośrednio od tej osoby.

2. Wraz z informacją, o której mowa w ust. 1, osobie, której dane dotyczą dostarcza się kopę Danych Osobowych podlegających przetwarzaniu. Kopia przekazywana jest poprzez e-mail, chyba że zainteresowany we wniosku wskaże inną formę.
3. Za wszelkie kolejne kopie, o które zwróci się osoba w przeciągu 30 dni od otrzymania poprzedniej kopii, ADO pobiera opłatę w wysokości odpowiadającej kosztom administracyjnym poniesionym przez ADO w związku ze sporządzeniem takiej kopii.

5.4 Prawo do sprostowania danych

1. ADO dokłada wszelkich starań w celu zapewnienia poprawności Przetwarzanych Danych Osobowych.
2. Na wniosek zainteresowanego ADO zobowiązany jest do niezwłocznego sprostowania dotyczących go Danych Osobowych, które są nieprawidłowe.
3. Biorąc pod uwagę cele przetwarzania oraz zasadę minimalizacji Danych Osobowych, ADO na żądanie zainteresowanego uzupełnia niekompletne Dane Osobowe albo odmawia takiego uzupełnienia, jeżeli jest to zbędne przy uwzględnieniu celu przetwarzania danych.

5.5 Prawo do usunięcia danych oraz prawo do ograniczenia przetwarzania

1. ADO zobowiązany jest od usunięcia lub ograniczenia przetwarzania Danych Osobowych w sytuacjach wskazanych w Rozporządzeniu lub innych obowiązujących przepisach.
2. W terminie określonym w pkt 5.1 ppkt 7 niniejszej Polityki Ochrony Danych Osobowych, ADO dokonuje weryfikacji i zasadności zgłoszonego przez uprawnionego wniosku oraz podejmuje decyzję:
   a) o wykonaniu żądania zgodnie z wnioskiem zainteresowanego albo
   b) o odmowie wykonania żądania, w szczególności ze względu na okoliczności wskazane w art. 17 ust. 3 Rozporządzenia.
3. Do czasu rozpatrzenia wniosku o ograniczenie przetwarzania, ADO niezwłocznie, nie później niż w ciągu dwóch dni roboczych od otrzymania wniosku, zaprzestaje przetwarzania danych osobowych, za wyjątkiem przechowywania.
4. W razie pozytywnego rozpatrzenia wniosku o usunięcie danych, ADO w ciągu dwóch dni roboczych godzin usuwa wszystkie Przetwarzane Dane Osobowe, za wyjątkiem danych, które musi dalej przetwarzać w celu ustalenia, dochodzenia lub obrony ewentualnych roszczeń.
5. W razie pozytywnego rozpatrzenia wniosku o ograniczenie przetwarzania danych ADO w ciągu dwóch dni roboczych od złożenia wniosku zaprzestaje przetwarzania tych danych za wyjątkiem ich przechowania lub przetwarzania niezbędnego do celu ustalenia, dochodzenia lub obrony ewentualnych roszczeń. Dalsze Przetwarzanie Danych Osobowych jest także możliwe za zgodą osoby, której dane dotyczą lub w celu ochrony praw innej osoby fizycznej lub prawnej.
6. ADO ma prawo do zaprzestania świadczenia usług, jeżeli dalsze ich świadczenie jest niemożliwe ze względu na usunięcie lub ograniczenie przetwarzania Danych Osobowych, o czym informuje zainteresowanego wraz z informacją o rozpatrzeniu wniosku. W taki sam sposób ADO informuje o uchyleniu ograniczenia Przetwarzania Danych Osobowych.

5.6 Prawo do przenoszenia Danych Osobowych

1. ADO zobowiązany jest do przekazania zainteresowanemu danych osobowych go dotyczących, pod warunkiem że:
   a) Dane Osobowe zostały dostarczone przez zainteresowanego;
   b) Przetwarzanie Danych Osobowych odbywa się na podstawie zgody zainteresowanego lub jest niezbędne do wykonania umowy, której stroną jest zainteresowany albo do podjęcia działań na żądanie zainteresowanego przed zawarciem umowy.

c) Przetwarzanie Danych Osobowych odbywa się w sposób zautomatyzowany.

2. Dane Osobowe są przekazywane w formacie pliku excel.
3. Dane osobowe są przekazywane zainteresowanemu lub, na jego wniosek, innemu administratorowi. W przypadku przekazywania Danych Osobowych innemu administratorowi, zainteresowany jest zobowiązany podać dane identyfikujące odbiorcę danych wystarczające do przekazania tych danych, w tym w szczególności:
   a) nazwę odbiorcy danych;
   b) adres, w tym adres e-mail, na który mają zostać wysłane Dane osobowe.
4. Po przekazaniu danych ADO, w ciągu siedmiu dni roboczych, usuwa wszystkie Przetwarzane Dane osobowe, za wyjątkiem danych, które ADO musi przetwarzać w dalszym ciągu do celu ewentualnego ustalenia, dochodzenia, obrony roszczeń lub jest do tego zobowiązany nad podstawie przepisów prawa.

5.7 Prawo do wniesienia sprzeciwu

1. Zainteresowany ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jego Danych Osobowych opartego na art. 6 ust. 1 e) i f) RODO, to jest gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub gdy jest ono niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią.
2. Jeżeli Zainteresowany zgłosi sprzeciw wobec przetwarzania jego Danych osobowych do celów marketingu bezpośredniego, administrator zaprzestaje przetwarzać dane osobowe do tego celu
3. W razie pozytywnego rozpatrzenia sprzeciwu, Administrator w ciągu siedmiu dni roboczych usuwa wszystkie Przetwarzane Dane osobowe, za wyjątkiem danych, które administrator musi przetwarzać w dalszym ciągu do celu ewentualnego ustalenia, dochodzenia lub obrony roszczeń lub gdy wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności zainteresowanego.
4. O prawie do wniesienia sprzeciwu Zainteresowany jest informowany najpóźniej przy okazji pierwszej komunikacji z nim w sposób wyraźny, w formie odpowiadającej sposobowi komunikacji z Zainteresowanym.

6 ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

6.1 Podstawowe zasady

1. Za bieżącą, operacyjną ochronę Danych Osobowych odpowiada każda osoba przetwarzająca te dane w ramach jej obowiązków służbowych oraz roli sprawowanej w procesie Przetwarzania Danych Osobowych.
2. Każda z osób mająca styczność z Danymi Osobowymi jest zobowiązana do ich ochrony oraz Przetwarzania Danych Osobowych w granicach udzielonego jej upoważnienia.
3. Osoby przetwarzające Dane Osobowe powinny stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa Przetwarzania Danych Osobowych.

6.2 Procedury postępowania z Danymi Osobowymi

1. Dostęp do Danych Osobowych powinien być przyznawany tylko osobom, którym taki dostęp jest niezbędny do wykonywania ich obowiązków lub zapewnienia ochrony Danych Osobowych.
2. Dane Osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
3. Dane Osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
4. Osoby Upoważnione mają obowiązek podejmowania wszelkich działań mających na celu ochronę Danych Osobowych oraz stosowania procedur ochrony Danych Osobowych, a w szczególności:
   a) stosowania haseł dostępowych;

b) powstrzymywania się od drukowania i kopiowania dokumentów bez wyraźnej potrzeby;
c) nie wynoszenia bez wyraźnej potrzeby dokumentów poza miejsce, w którym są one przechowywane;
d) pozostawiania Stacji Roboczej z zablokowanym ekranem;
e) niepozostawiania dokumentów bez nadzoru;
f) bezzwłocznego usuwania z dysku niepotrzebnych danych/dokumentów;
g) bezzwłocznego fizycznego niszczenia, uniemożliwiającego odczyt, niepotrzebnych drukowanych dokumentów;
h) bezzwłocznego usuwania zbędnych danych i dokumentów z przenośnych nośników;
i) odpowiedniego zabezpieczenia Danych Osobowych wysyłanych drogą e-mail.

6.3 Upoważnienie do Przetwarzania Danych Osobowych

1. Do Przetwarzania Danych Osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO.
2. Upoważnienia są wydawane przed rozpoczęciem Przetwarzania Danych Osobowych, z uwzględnieniem zasady minimalizacji danych.
3. Upoważnienie jest wydawane po dostarczeniu ADO podpisanego Oświadczenia, którego wzór stanowi **Załącznik nr 3** do niniejszej Polityki Przetwarzania Danych Osobowych.
4. Upoważnienie sporządzane jest wg wzoru stanowiącego **Załącznik nr 4** do niniejszej Polityki Przetwarzania Danych Osobowych.
5. Upoważnienia przechowywane są w aktach Osobowych pracowników i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z Przetwarzaniem Danych Osobowych.

6.4 Ewidencja Osób Upoważnionych

1. Ewidencja Osób Upoważnionych do Przetwarzania Danych Osobowych jest prowadzona przez ADO i zawiera:
   a) imię i nazwisko Osoby Upoważnionej;
   b) zakres upoważnienia;
   c) identyfikator, jeśli Osoba Upoważniona została zarejestrowana w Systemie Informatycznym służącym do Przetwarzania Danych Osobowych;
   d) datę nadania i wygaśnięcia uprawnień.
2. Przełożeni Osób Upoważnionych odpowiadają za natychmiastowe zgłoszenie do ADO osób, które utraciły uprawnienia dostępu do Danych Osobowych.

6.5 Znajomości regulacji wewnętrznych

Osoby Upoważnione do Przetwarzania Danych Osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony Danych Osobowych w Izbie, w szczególności z Polityką Ochrony Danych Osobowych.

ADO informuje na bieżąco Osoby Upoważnione o obowiązkach spoczywających na nich na mocy Rozporządzenia, Ustawy oraz innych obowiązujących przepisów.

W razie jakichkolwiek wątpliwości dotyczących Przetwarzania Danych Osobowych, Osoby Upoważnione mogą zwrócić się do ADO o wyjaśnienia i poradę.

6.6 Zgodność Polityki Ochrony Danych Osobowych z przepisami

1. Niniejsza Polityka Ochrony Danych Osobowych podlega aktualizacji wraz ze zmieniającymi się przepisami prawnymi o ochronie danych Osobowych oraz zmianami faktycznymi w Izbie, które mogą

powodować, że zasady Ochrony Danych Osobowych określone w obowiązujących dokumentach są nieaktualne lub nieadekwatne.

2. Okresowy przegląd Polityki Ochrony Danych Osobowych ma na celu stwierdzenie, czy jej postanowienia odpowiadają aktualnej i planowanej działalności Izby, oraz aktualnemu stanowi prawnemu. Przegląd przeprowadzany jest przez ADO co najmniej raz na rok oraz w razie istotnych zmian w obowiązujących przepisach prawa.
3. Każda zmiana Polityki Ochrony Danych Osobowych będzie skutkowała przeglądem i aktualizacją innych procedur dotyczących ochrony Danych Osobowych obowiązujących w Izbie.

7 ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

7.1 Bezpieczeństwo usług zewnętrznych

Osoby zamawiające w imieniu ADO usługi u podmiotów zewnętrznych oraz odpowiedzialne za realizację tych usług są obowiązane zapewnić, aby:

a) usługi były realizowane zgodnie z wymaganiami bezpieczeństwa Przetwarzania Danych Osobowych obowiązującymi w Spółce, wymaganiami umowy oraz wymaganiami prawa,
b) umowa o świadczeniu usług określała wymagania bezpieczeństwa Przetwarzania Danych Osobowych, zakres ich przetwarzania oraz sposób ich przekazywania;
c) podmioty świadczące usługi zapewniały wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by Przetwarzanie Danych Osobowych spełniało wymogi Rozporządzenia oraz chroniło prawa osób, których dane dotyczą.

7.2 Powierzanie Przetwarzania Danych Osobowych

1. Powierzenie Przetwarzania Danych Osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności przedmiot i czas trwania Przetwarzania Danych Osobowych, charakter i cel przetwarzania, rodzaj Danych Osobowych oraz kategorie osób, których dane dotyczą oraz obowiązki i zakres odpowiedzialności podmiotu, któremu powierzono Przetwarzanie Danych Osobowych, z tytułu niewykonania lub nienależytego wykonania umowy.
2. Powierzenie Przetwarzania Danych Osobowych musi uwzględniać wymogi określone w art. 28 Rozporządzenia. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone Przetwarzanie Danych Osobowych, jest obowiązany przed rozpoczęciem Przetwarzania Danych Osobowych do podjęcia środków wymaganych na mocy art. 32 Rozporządzenia.
3. W umowach stanowiących podstawę powierzenia Przetwarzania Danych Osobowych należy umieścić zobowiązanie podmiotu zewnętrznego do Przetwarzania danych Osobowych wyłącznie na udokumentowane polecenie ADO.
4. Podmiot Przetwarzający Dane Osobowe nie może korzystać z usług innego podmiotu przetwarzającego bez uzyskania uprzedniej szczegółowej lub ogólnej pisemnej zgody ADO. W przypadku ogólnej pisemnej zgody podmiot przetwarzający zobowiązany jest do informowania ADO o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, umożliwiając ADO wyrażenie sprzeciwu wobec takich zmian.
5. Powierzenie Przetwarzania Danych Osobowych nie oznacza zwolnienia Izby z odpowiedzialności za zgodne z prawem Przetwarzanie Danych Osobowych, co oznacza konieczność zapewnienia Izbie uprawnienia do przeprowadzenia w siedzibie podmiotu zewnętrznego kontroli wykonania umowy stanowiącej podstawę powierzenia Przetwarzania Danych Osobowych m. in. w zakresie obowiązujących regulacji wewnętrznych, udzielonych Upoważnień do przetwarzania danych oraz nałożonych zobowiązań do zachowania tajemnicy. Podmiot zewnętrzny powinien także udostępnić ADO wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Rozporządzeniu.

6. Podmiot, któremu powierzono Przetwarzanie danych Osobowych może być w miarę możliwości zobowiązany do posiadania ubezpieczenia odpowiedzialności cywilnej za szkody spowodowane nieprawidłowym przetwarzaniem powierzonych Danych Osobowych.

7.3 Udostępnianie Danych Osobowych

1. Dane Osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dane dotyczą.
2. Udostępnianie Danych Osobowych może nastąpić **wyłącznie za zgodą ADO.**
3. Dane Osobowe mogą być udostępniane wyłącznie z uwzględnieniem zasad ich bezpieczeństwa, w tym w szczególności zasady minimalizacji danych.
4. Informacje zawierające Dane Osobowe powinny być przekazywane uprawnionym podmiotom lub osobom listem poleconym za potwierdzeniem odbioru lub w inny bezpieczny sposób, w tym za pośrednictwem systemu informatycznego.
5. Udostępniając Dane Osobowe innym podmiotom, ADO ma obowiązek odnotowywać informacje o udostępnieniu bezpośrednio w Systemie Informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy Danych Osobowych oraz datę i zakres udostępnionych Danych Osobowych.
6. Udostępniając Dane Osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
7. Zasady udostępniania Danych Osobowych osobie, której dane dotyczą, zostały określone w pkt. 5 powyżej.

8 BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

8.1 Obszary Przetwarzania Danych Osobowych

1. Dane Osobowe mogą być przetwarzane wyłącznie w pomieszczeniach biurowych gdzie Izba prowadzi działalność, a także poza nimi w trakcie podróży służbowych (na zasadach określonych w pkt. 8.4 poniżej). Do takich pomieszczeń zalicza się w szczególności:
   a) pomieszczenia biurowe, w których zlokalizowane są Stacje Robocze lub serwery służące do Przetwarzania Danych Osobowych,
   b) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z Systemu Informatycznego oraz korespondencję zawierającą Dane Osobowe,
   c) pomieszczenia, w których przechowywane są urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające Dane Osobowe.
2. Pomieszczenia, w których przetwarzane są Dane Osobowe, powinny być zamykane podczas nieobecności Osób Upoważnionych, w sposób wyłączający możliwość dostępu do nich osób nieupoważnionych.
3. Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są Dane Osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy jak i po jej zakończeniu i właściwego zabezpieczenia kluczy. Nie można wynosić ww. kluczy poza miejsca przeznaczone do ich przechowywania.
4. Wydruki i nośniki elektroniczne zawierające Dane Osobowe należy przechowywać w zamykanych na klucz szafach, które znajdują się w obszarach Przetwarzania Danych Osobowych.
5. Niepotrzebne wydruki lub inne dokumenty należy niezwłocznie niszczyć za pomocą niszczarek lub wrzucać do specjalnych pojemników na dokumenty przeznaczone do zniszczenia.

8.2 Bezpieczeństwo środowiskowe

1. Lokalizację Danych Osobowych należy starannie dobierać z uwzględnieniem wymaganych aspektów bezpieczeństwa Przetwarzania Danych Osobowych. W szczególności należy rozważyć aspekty dotyczące:
   a) nieprzerwanego zasilania energią elektryczną;
   b) klimatyzacji oraz wentylacji;
   c) ochrony przed pożarem i zalaniem;
   d) fizycznej kontroli dostępu.
2. Pomieszczenia wchodzące w skład obszaru Przetwarzania Danych Osobowych należy wyposażyć w odpowiednie środki ochrony fizycznej przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.
3. Kopie zapasowe zawierające Dane Osobowe powinny być (w miarę możliwości lokalizacyjnych) przechowywane w drugiej fizycznej lokalizacji w bezpiecznej odległości od lokalizacji podstawowej.

8.3 Bezpieczeństwo urządzeń

1. Urządzenia służące do Przetwarzania Danych Osobowych należy przechowywać w bezpieczny i nadzorowany sposób.
2. Urządzenia mobilne takie, jak komputery przenośne, urządzenia mobilne, telefony komórkowe, nie powinny być pozostawiane bez opieki, jeżeli nie są zastosowane odpowiednie środki ochrony przed dostępem osób nieuprawnionych.

8.4 Zasady zabezpieczania komputerów przenośnych, na których są przetwarzane Dane Osobowe

1. Przetwarzanie Danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków.
2. Komputer przenośny, na którym przetwarzane są Dane Osobowe, powinien zostać zabezpieczony w taki sposób, że:
   a) dokonano konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł,
   b) dokonano instalacji i konfiguracji oprogramowania antywirusowego,
   c) przeprowadzono aktualizację bazy wirusów zgodnie z zasadami zarządzania programem antywirusowym.
3. Komputery przenośne, mogą być wynoszone przez pracownika poza miejsce pracy, jeżeli, spełnione są wszystkie zalecenia z pkt 2.
4. Komputery przenośne, które wykorzystywane są do Przetwarzania Danych Osobowych wyłącznie w miejscu pracy, nie muszą spełniać wymogów pkt 2 lit. b).
5. W razie zgubienia lub kradzieży komputera przenośnego, na którym przetwarzane są Dane Osobowe, pracownik zobowiązany jest do natychmiastowego powiadomienia ADO.

8.5 Fizyczna kontrola dostępu

1. Należy przestrzegać zasady „czystego biurka” i „czystego ekranu” w celu zredukowania ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia Danych Osobowych.
2. Pobyt w pomieszczeniach, w których znajdują się Systemy Informatyczne służące do Przetwarzania Danych Osobowych, osób nieupoważnionych, w tym gości ADO, powinien być nadzorowany przez cały czas pobytu tych osób.
3. Dostęp do systemów komputerowych, w których przetwarzane są Dane Osobowe oraz do pomieszczeń, w których znajdują się archiwa dokumentów lub przechowywane są kopie zapasowe, mogą mieć wyłącznie osoby upoważnione.
4. Kontrolą dostępu do obszarów przeznaczonych do Przetwarzania Danych Osobowych zajmuje się ADO.
5. Przyznawanie dostępu gościom Izby może się odbywać wyłącznie w określonych i uzasadnionych celach.

6. Przed zakończeniem pracy należy zabezpieczyć stanowisko pracy, w szczególności wyłączyć komputer oraz zabezpieczyć wszelką dokumentację, wydruki, elektroniczne zewnętrzne nośniki informacji (np. zewnętrzne dyski twarde, płyty CD/DVD, pendrive'y) i umieścić je w zamykanych szafkach.
7. Monitory należy ustawić w taki sposób, aby uniemożliwić osobom nieuprawnionym podgląd wyświetlanych Danych Osobowych.
8. W przypadku korzystania z usług zewnętrznych podmiotów oferujących zbieranie i niszczenie dokumentów, urządzeń lub nośników zawierających Dane Osobowe należy wybrać wykonawcę z odpowiednimi uprawnieniami, zabezpieczeniami i doświadczeniem.

9 ZARZĄDZANIE INCYDENTAMI

9.1 Monitorowanie incydentów

1. Incydenty związane z bezpieczeństwem Przetwarzania Danych Osobowych po ich wykryciu powinny być niezwłocznie rejestrowane i monitorowane w celu ich właściwego zidentyfikowania i podjęcia działań zapobiegających rozszerzeni ich negatywnych skutków.
2. Informacje o zdarzeniach systemowych powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem Przetwarzania Danych Osobowych.
3. Użytkownicy Systemów powinni znać i przestrzegać zasad zgłaszania incydentów związanych z bezpieczeństwem Przetwarzania Danych Osobowych.

9.2 Opis zdarzeń naruszających ochronę Danych Osobowych

1. Zagrożenia losowe dla Danych Osobowych można podzielić na:
   a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności Danych Osobowych, ich zniszczenia i uszkodzenia infrastruktury technicznej Systemu Informatycznego – może zostać zakłócona ciągłość pracy Systemu Informatycznego, może nastąpić naruszenie poufności Danych Osobowych;
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki, awarie sprzętowe, błędy oprogramowania), wskutek których może dojść do zniszczenia Danych Osobowych, może zostać zakłócona ciągłość pracy Systemu Informatycznego lub może nastąpić naruszenie poufności Danych Osobowych.
2. Zagrożenia mogą być też zamierzone, świadome i celowe; najpoważniejsze zagrożenia naruszenia poufności Danych Osobowych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy) dzieli się na:
   a) nieuprawniony dostęp do Systemu Informatycznego z zewnątrz (włamanie);
   b) nieuprawniony dostęp do Systemu Informatycznego spowodowany przez pracownika;
   c) nieuprawnione przekazanie Danych Osobowych;
   d) pogorszenie jakości Systemu Informatycznego skutkujące utratą lub obniżeniem poziomu ochrony poufności.
3. Naruszenie lub podejrzenie naruszenia zabezpieczenia Systemu informatycznego, w którym przetwarzane są Dane osobowe, to głównie:
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
   b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;

c) awaria Systemu informatycznego, która wyraźnie wskazuje na umyślne działanie w celu naruszenia Ochrony Danych Osobowych lub sabotaż, a także niewłaściwe działanie serwisu, a w tym pozostawienia serwisantów bez nadzoru;
d) pojawienie się komunikatu alarmowego w tej części Systemu informatycznego, która zapewnia ochronę zasobów lub innego komunikatu o podobnym znaczeniu;
e) jakość Danych Osobowych w Systemie informatycznym lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia Systemu lub inną nadzwyczajną i niepożądaną ingerencję lub modyfikację w Systemie;
f) naruszenie lub próba naruszenia integralności Systemu informatycznego lub bazy danych w tym Systemie;
g) potwierdzona próba lub modyfikacja Danych Osobowych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
h) niedopuszczalna manipulacja Danymi Osobowymi w Systemie informatycznym;
i) ujawnienie osobom nieupoważnionym Danych Osobowych lub objętych tajemnicą procedur ochrony Przetwarzania Danych Osobowych albo innych elementów systemu zabezpieczeń;
j) praca w Systemie informatycznym lub sieci komputerowej wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy i wskazująca 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.;
k) ujawnienie istnienia nieautoryzowanych kont dostępu do Danych Osobowych lub tzw. "bocznej furtki" itp.;
l) podmiana lub zniszczenie nośników z Danymi Osobowymi bez odpowiedniego upoważnienia lub niedozwolone skasowanie albo skopiowanie Danych Osobowych;
m) 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 terminie kopii bezpieczeństwa, praca na Danych Osobowych w celach prywatnych itp.).

4. Za naruszenie Ochrony Danych Osobowych uważa się również stwierdzone 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, dyskietkach w formie niezabezpieczonej itp.

9.3 Zgłaszanie incydentów

1. Osoby Upoważnione biorące udział w Przetwarzaniu Danych Osobowych w Systemie Informatycznym są odpowiedzialne za bezpieczeństwo tych danych. Każda osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia Ochrony Danych Osobowych lub mogące spowodować naruszenie bezpieczeństwa, zobowiązana jest do natychmiastowego poinformowania ADO.
2. O naruszeniu Ochrony Danych osobowych mogą świadczyć następujące symptomy:
   a) brak możliwości uruchomienia lub wyłączenia przez użytkownika Systemu aplikacji pozwalającej na dostęp do Danych osobowych;
   b) brak możliwości zalogowania się do tej aplikacji, ograniczone w stosunku do normalnej sytuacji uprawnienia użytkownika Systemu w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
   c) wygląd aplikacji inny niż normalnie;

d) inny zakres danych niż normalnie dostępny dla użytkownika Systemu Informatycznego– dużo więcej lub dużo mniej danych;
e) znaczne spowolnienie działania Systemu Informatycznego;
f) pojawienie się niestandardowych komunikatów generowanych przez System Informatyczny;
g) ślady włamania lub prób włamania do obszaru lub pomieszczeń, w których przetwarzane są Dane Osobowe, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych;
h) włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub innej – nośniki Danych Osobowych;
i) zagubienie bądź kradzież nośnika Danych Osobowych lub nośnika materiału kryptograficznego (karty mikroprocesorowej, pendrive, itp.);
j) kradzież sprzętu informatycznego, w którym przechowywane są Dane Osobowe;
k) informacja z systemu antywirusowego o zainfekowaniu Systemu Informatycznego wirusami;
l) fizyczne zniszczenie lub podejrzenie zniszczenia elementów Systemu Informatycznego;
m) celowe działania albo zaistnienie działań siły wyższej, podejrzenie nieautoryzowanej modyfikacji Danych Osobowych przetwarzanych w Systemie Informatycznym.

3. W wypadku stwierdzenia naruszenia bezpieczeństwa Danych Osobowych należy natychmiast powiadomić ADO. Informacja o pojawieniu się zagrożenia jest przekazywana przez Osobę Upoważnioną osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż ADO, jest ona zobowiązana natychmiast poinformować o tym fakcie ADO.
4. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w Spółce naruszenia bezpieczeństwa Danych Osobowych ADO jest zobowiązany do podjęcia działań w celu:
   a) wyjaśnienia zdarzenia, a w szczególności, czy miało miejsce naruszenie zasad ochrony Danych Osobowych,
   b) wyjaśnienia przyczyn naruszenia i zebrania ewentualnych dowodów naruszenia zasad ochrony Danych Osobowych, a w szczególności ustalenia, czy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
   c) zabezpieczenia Systemu Informatycznego przed powiększeniem się zagrożenia;
   d) przywrócenia pierwotnego stanu Systemu Informatycznego (to jest stanu sprzed incydentu) oraz usunięcia skutków incydentu.
5. ADO podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia poprzez:
   a) przeprowadzenie analizy poprawności funkcjonowania Systemu Informatycznego,
   b) weryfikację sposobów zabezpieczenia przetwarzania danych w Systemie Informatycznym, w szczególności danych konfiguracyjnych tego Systemu Informatycznego.
6. Na podstawie zebranych informacji ADO określa przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, ADO powinien poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa Danych Osobowych.
7. System Informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia skutków incydentu.
8. ADO prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa Danych Osobowych. Ewidencja taka obejmuje następujące informacje:
   a) imię i nazwisko osoby zgłaszającej incydent,
   b) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
   c) datę zgłoszenia incydentu,

d) okoliczności naruszenia Ochrony Danych Osobowych,
e) skutki naruszenia Ochrony Danych Osobowych,
f) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
g) wyniki przeprowadzonych działań,
h) podjęte akcje naprawcze i ocena ich skuteczności.

9. ADO jest odpowiedzialny za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:
   a) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
   b) określenia wymaganych działań zwiększających bezpieczeństwo Systemu Informatycznego i minimalizujących ryzyko zaistnienia incydentów,
   c) określenia potrzeb w zakresie szkoleń Osób Upoważnionych.

9.4 Zgłaszanie naruszeń UODO

1. W przypadku naruszenia Ochrony Danych Osobowych ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je UODO.
2. Zgłoszenia nie dokonuje się, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Jeżeli zgłoszenie zostanie dokonane po upływie 72 godzin od stwierdzenia naruszenia, do zgłoszenia UODO dołącza się wyjaśnienie przyczyn opóźnienia.

10 POSTANOWIENIA KOŃCOWE

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Ochrony Danych Osobowych może być podstawą rozwiązania stosunku pracy lub innej umowy z osobą, która dopuściła się zawinionego naruszenia tych zasad.
2. Przypadki nieuzasadnionego zaniechania realizacji obowiązków wynikających z Polityki Ochrony Danych Osobowych lub naruszenia tych obowiązków mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności gdy pracownik w razie naruszenia zasad ochrony Danych Osobowych lub uzasadnionego podejrzenia takiego naruszenia nie powiadomił o tym ADO. Kara dyscyplinarna orzeczona wobec takiego pracownika nie wyklucza jego odpowiedzialności karnej zgodnie z Ustawą oraz odpowiedzialności odszkodowawczej wobec ADO.
3. W sprawach nieuregulowanych w Polityce Ochrony Danych Osobowych mają zastosowanie przepisy Rozporządzenia, Ustawy oraz przepisy wykonawcze do Ustawy.
4. Pracownicy Izby w szczególności Osoby Upoważnione, zobowiązani są do stosowania przy Przetwarzaniu Danych Osobowych postanowień zawartych w niniejszej Polityce Przetwarzania i Ochrony Danych Osobowych. W przypadku odrębnych uregulowań występujących w innych procedurach obowiązujących w Spółce użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony Danych Osobowych.
5. Załączniki do niniejszej Polityki Ochrony Danych Osobowych stanowią jej integralną część i obejmują:
   1.1 **Załącznik nr 1** – Rejestr czynności przetwarzania;
   1.2 **Załącznik nr 2** – Analiza ryzyka przetwarzania Danych Osobowych;
   1.3 **Załącznik nr 3**- Oświadczenie o przestrzeganiu przepisów o ochronie Danych Osobowych;
   1.4 **Załącznik nr 3a** – Oświadczenie o przestrzeganiu przepisów o ochronie Danych Osobowych przez pracownika firmy zewnętrznej;
   1.5 **Załącznik nr 4** – Upoważnienie do Przetwarzania Danych Osobowych;

1.6 **Załącznik nr 4a** – Upoważnienie do Przetwarzania Danych Osobowych dla pracowników firm zewnętrznych.

6. Niniejsza Polityka Ochrony Danych Osobowych wchodzi w życie z dniem 8 października 2018 roku i zostanie ogłoszona wszystkim pracownikom Izby zgodnie z zasadami przyjętymi w Izbie.

ZAŁĄCZNIK NR 1

Rejestr czynności przetwarzania Danych Osobowych

w Izbie Gospodarczej Handlowców, Przetwórców Zbóż i Producentów Pasz

1. ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych osobowych jest Izba Gospodarcza Handlowców, Przetwórców Zbóż i Producentów Pasz z siedzibą w Warszawie przy ul. Wspólnej 56, 00-684 Warszawa, NIP: 5272102616, KRS: 0000116407, REGON: 012969507.

2. CELE I KATEGORIE PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	1.	2.	3.	4.	5.	6.
Kategoria osób, których Dane Osobowe dotyczą	**pracownicy i współpracownicy**	**byli pracownicy i współpracownicy**	**kandydaci do pracy**	**kontrahenci oraz osoby reprezentujące kontrahentów – przedsiębiorców**	**członkowie rady Izby i innych organów Izby**	**osoby reprezentujące członków Izby**
Kategoria Danych Osobowych	dane związane z zatrudnieniem, w tym dane zawarte w aktach osobowych oraz wizerunek pracownika	dane związane z zatrudnieniem, w tym dane zawarte w aktach osobowych oraz wizerunek pracownika	dane podawane zgodnie z kodeksem pracy lub – w przypadku zatrudnienia na innej podstawie: imię i nazwisko; datę urodzenia; numer telefonu; adres e-mail; adres do korespondencji	dane kontaktowe, w tym: imię i nazwisko; numer telefonu; adres e-mail	imię i nazwisko; numer PESEL,	imię i nazwisko; stanowisko
Sposób pozyskiwania Danych Osobowych	dobrowolnie, za pomocą kwestionariusza osobowego bezpośrednio od osoby, której dane dotyczą	dobrowolnie, za pomocą kwestionariusza osobowego bezpośrednio od osoby, której dane dotyczą	dobrowolnie, cv	dobrowolnie, w trakcie zawierania umowy	dobrowolnie, w trakcie rozpoczęcia współpracy	dobrowolnie, w trakcie rozpoczęcia współpracy
Cel przetwarzania Danych Osobowych	zatrudnienie	zatrudnienie	zatrudnienie	prowadzenie działalności biznesowej	prowadzenie działalności biznesowej	prowadzenie działalności biznesowej
Podstawa prawna przetwarzania Danych Osobowych	art. 22[1] Kodeksu pracy i przepisy szczegółowe; Rozporządzenia; dane osobowe w postaci wizerunku zgoda podmiotu danych – art. 6 ust. 1 pkt a) Rozporządzenia	art. 22[1] Kodeksu pracy i przepisy szczegółowe; Rozporządzenia; art. 6 ust. 1 pkt c) Rozporządzenia	Art. 22 § 1 Kodeksu pracy; art. 6 ust. 1 pkt a) Rozporządzenia	art. 6 ust. 1 pkt b) Rozporządzenia	art. 6 ust. 1 pkt a) Rozporządzenia	art. 6 ust. 1 pkt a) Rozporządzenia
Kategorie osób (działy, stanowiska) upoważnionych do przetwarzania Danych Osobowych	Prezydent / Sekretarz Generalny / księgowość	Prezydent / Sekretarz Generalny / księgowość	Prezydent / Sekretarz Generalny / Prezydium / Komisja rekrutacyjna	Prezydent / Sekretarz Generalny / Pracownicy biura IZP/ księgowość	Prezydent / Sekretarz Generalny / Pracownicy biura IZP/ księgowość	Prezydent / Sekretarz Generalny / Pracownicy biura IZP/ księgowość
Kategorie podmiotów, którym Dane	Dane mogą być powierzane podmiotom świadczącym na	Dane mogą być powierzane podmiotom świadczącym na	-	Dane mogą być powierzane podmiotom świadczącym na	Dane mogą być powierzane podmiotom świadczącym na	Dane mogą być powierzane podmiotom świadczącym na

Osobowe mogą być udostępniane	rzecz Izby usługi związane z zatrudnianiem i przywilejami pracowników, w tym w zakresie obsługi wynagrodzeń	rzecz Izby usługi związane z zatrudnianiem i przywilejami pracowników, w tym w zakresie obsługi wynagrodzeń		rzecz Izby usługi związane z rozliczeniami finansowo-księgowymi	rzecz Izby usługi związane z rozliczeniami finansowo-księgowymi	rzecz Izby usługi związane z rozliczeniami finansowo-księgowymi
Kategorie podmiotów, którym Dane Osobowe mogą być powierzone	Dane mogą być powierzane podmiotom świadczącym na rzecz Izby usługi związane z zatrudnianiem i przywilejami pracowników, w tym w zakresie obsługi wynagrodzeń	Dane mogą być powierzane podmiotom świadczącym na rzecz Izby usługi związane z zatrudnianiem i przywilejami pracowników, w tym w zakresie obsługi wynagrodzeń	-	Dane mogą być powierzane podmiotom świadczącym na rzecz Izby usługi związane z rozliczeniami finansowo-księgowymi	Dane mogą być powierzane podmiotom świadczącym na rzecz Izby usługi związane z rozliczeniami finansowo-księgowymi	Dane mogą być powierzane podmiotom świadczącym na rzecz Izby usługi związane z rozliczeniami finansowo-księgowymi
Okres przetwarzania Dane Osobowe	Przez okres zatrudnienia (obowiązywania umowy) oraz po ustaniu zatrudnienia, przez okres wymagany przepisami prawa, w tym dotyczącymi przechowywania akt osobowych	Po ustaniu zatrudnienia, przez okres wymagany przepisami prawa, w tym dotyczącymi przechowywania akt osobowych	Przez okres prowadzenia danego postępowania rekrutacyjnego oraz przez dalszy okres – jeżeli kandydat wyraził zgodę na dalsze przetwarzanie jego Danych Osobowych	Przez okres obowiązywania umowy o współpracę oraz okres niezbędny do dokonania rozliczeń pomiędzy stronami po rozwiązaniu lub wygaśnięciu umowy	Przez okres członkostwa w Radzie Izby lub innym organie Izby	Przez okres członkostwa w Izbie
Informacja o ewentualnym przekazywaniu Dane Osobowe do państwa trzeciego	Dane Osobowe nie są przekazywane	Dane Osobowe nie są przekazywane	Dane Osobowe nie są przekazywane	Dane Osobowe nie są przekazywane	Dane Osobowe nie są przekazywane	Dane Osobowe nie są przekazywane
Data wpisu/modyfikacji wpisu	-	-	-	-	-	-
Data wykreślenia z rejestru						

ZAŁĄCZNIK NR 2

Analiza ryzyka Przetwarzania Danych Osobowych

w Izbie Gospodarczej Handlowców, Przetwórców Zbóż i Producentów Pasz

Działając, w imieniu spółki Izba Gospodarcza Handlowców, Przetwórców Zbóż i Producentów Pasz z siedzibą w Warszawie przy ul. Wspólnej 56, 00-684 Warszawa, NIP: 5272102616, KRS 0000116407, REGON: 012969507 („**Izba**"), na podstawie art. 35 i 36 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 (opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1) („**Rozporządzenie**"), oświadczam, iż Izba dokonała analizę ryzyka dla ochrony danych osobowych, po uprzedniej konsultacji z Inspektorem Ochrony Danych Osobowych Izby.
Analiza ryzyka w Izbie została przeprowadzona ze względu na rodzaj przetwarzania danych osobowych, ich charakter, zakres, kontekst i cele, z czym może wiązać się ryzyko naruszenia praw osób, których dane te dotyczą.

KATEGORIA	LP	ZAKRES	TAK	NIE	N/A	UWAGI
System zarządzania	1.	Czy został powołany inspektor ochrony danych (IOD)?		X		Izba nie ma obowiązku prawnego powołania IOD.
	2.	Czy została opracowana i wdrożona dokumentacja dotycząca ochrony danych i bezpieczeństwa?	X			
	3.	Czy osoby, które przetwarzają dane osobowe podpisały umowy o zachowaniu poufności?	X			
	4.	Czy osobom, które przetwarzają dane osobowe, nadane zostały upoważnienia do przetwarzania danych osobowych?	X			
	5.	Czy wymieniona powyżej dokumentacja jest aktualizowana?	X			
	6.	Kiedy miała miejsce ostatnia aktualizacja dokumentacji?				Październik 2018
	7.	Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych?	X			
	8.	Czy dla osób, które przetwarzają dane osobowe, organizowane są cykliczne szkolenia?	X			Tak, Izba ma przeprowadziła szkolenie w dniu 5 października 2018 roku.
	9.	Czy opracowano i wdrożono system zgłaszania nieprawidłowości z zakresie naruszenia danych osobowych?	X			
	10.	Czy wykonywane są okresowo audyty zgodności z przepisami prawa w zakresie danych osobowych?			X	Tak, Izba ma zamiar przeprowadzać audyt raz na pięć lat.
	11.	Czy wykonywane są audyty bezpieczeństwa np. dla systemów informatycznych lub testy penetracyjne?			X	Tak, Izba ma zamiar przeprowadzać audyt raz na pięć lat.
	12.	Kiedy przeprowadzane były ostatnie audyty?	X			Październik 2018
Odpowiednie przetwarzanie	13.	Czy dane osobowe przetwarzane są z uwzględnieniem wymagań przewidzianych przez przepisy prawa?	X			

Zniszczenie danych	14.	Czy dane osobowe są usuwane niezwłocznie po rozwiązaniu umowy powierzenia przetwarzania danych osobowych lub osiągnięciu celu przetwarzania?	X			
Umowa powierzenia przetwarzania	15.	Czy z podmiotami, którym zlecono przetwarzanie danych osobowych, zawarto umowy powierzenia przetwarzania danych?	X			
	16.	Czy umowy powierzenia przetwarzania danych osobowych zawierają następujące elementy:				
	a)	zakaz przetwarzania danych osobowych w celu innym niż określony w umowie;	X			
	b)	zostały określone techniczne i organizacyjne środki ochrony danych osobowych;	X			
	c)	cel przetwarzana danych został wyraźnie wskazany;	X			
	d)	zakaz dalszego powierzenia przetwarzania danych osobowych bez zgody administratora danych;	X			
	e)	stosowane są środki techniczne i organizacyjne mające na celu odpowiednie zabezpieczenie danych osobowych, które określone są w przepisach powszechnie obowiązującego prawa;	X			
	f)	wprowadzono odpowiedzialność z tytułu naruszeń zasad dotyczących przetwarzania danych osobowych;	X			
	g)	określono co stanie się z danymi po ustaniu umowy – zostaną usunięte lub zwrócone;	X			
	h)	zobowiązanie do informowania administratora o potencjalnych i stwierdzonych incydentach naruszenia ochrony danych osobowych;	X			
	i)	określone w RODO odnoszące się do umowy powierzenia przetwarzania danych osobowych?	X			
ŚRODKI TECHNICZE						
Uwierzytelnianie dostępu	17.	Czy dostęp do systemów informatycznych jest ograniczony zakresem zadań pracownika?	X			
	18.	Czy dostęp do systemów informatycznych, w ramach których przetwarzane są dane osobowe jest zmieniany wraz ze zmianą stanowiska pracownika lub likwidowany w razie jego odejścia z pracy?	X			
	19.	Czy pracownicy korzystają z indywidualnych kont użytkowników w systemie operacyjnym i systemach dedykowanych do przetwarzania danych?	X			
	20.	Czy opracowana i wdrożona została polityka zarządzania hasłami?	X			
	21.	Czy zainstalowano oprogramowanie antywirusowe?	X			

	22.	Czy użytkownicy mają uprawnienia do zmiany ustawień lub wyłączenia oprogramowania antywirusowego?		X		
	23.	Czy pracownicy mają zdalny dostęp do systemów informatycznych i dysków sieciowych?	X			
	24.	Czy zdalny dostęp ograniczony jest bezpiecznym połączeniem VPN?	X			
Ochrona przed wrogim oprogramowaniem	25.	Czy zainstalowane oprogramowanie ochronne odpowiada najbardziej aktualnej wersji?	X			
	26.	Czy oprogramowanie ochronne aktualizowane jest regularnie?	X			
	27.	Czy zagrożenie atakiem wrogiego oprogramowania monitorowane jest w czasie rzeczywistym?	X			
	28.	Czy użytkownicy mają uprawnienia do samodzielniej instalacji oprogramowania?		X		
Zabezpieczenia zewnętrzne	29.	Czy wszystkie komponenty składające się na system przetwarzania danych są aktualne? (Komponenty takie jak: System operacyjny, serwer aplikacji, serwer WWW, biblioteki zewnętrzne wykorzystane w kodzie aplikacji, i inne) • W przypadku pojawienia się krytycznych luk bezpieczeństwa, w wyniku których zdalny użytkownik może nielegalnie przejąć serwer, należy zastosować aktualizacje natychmiast. • W przypadku innych aktualizacji zabezpieczeń, należy ustalić regularny harmonogram aktualizacji, oraz audytowania				

ZAŁĄCZNIK NR 3
Oświadczenie o przestrzeganiu przepisów o ochronie Danych Osobowych
[WZÓR]

OŚWIADCZENIE

Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z:

- przepisów 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 (opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1) oraz polskiej ustawy o ochronie danych osobowych;
- Polityki Ochrony Danych Osobowych Izby Gospodarczej Handlowców, Przetwórców Zbóż i Producentów Pasz z siedzibą w Warszawie.

Zobowiązuję się do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie zatrudnienia w Izbie Gospodarczej Handlowców, Przetwórców Zbóż i Producentów Pasz z siedzibą w Warszawie jak również po ustaniu zatrudnienia.
Jednocześnie przyjmuję do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz powołanego powyżej Rozporządzenia.

……
Imię i nazwisko pracownika

Potwierdzam odbiór 1 egz. oświadczenia.

……
Data i czytelny podpis pracownika

ZAŁĄCZNIK NR 3A
Oświadczenie o przestrzeganiu przepisów o ochronie Danych Osobowych przez pracownika podmiotu zewnętrznego
[WZÓR]

OŚWIADCZENIE

Ja, niżej podpisany(a) zatrudniony(a) na umowę o pracę/ umowę zlecenia/ umowę o dzieło, w …… z siedzibą w ……, w związku z umową …… zawartą w dniu …… pomiędzy Izbą Gospodarczą Handlowców, Przetwórców Zbóż i Producentów Pasz oraz …… („**Umowa**"), oraz z przyznanymi mi uprawnieniami do przetwarzania danych osobowych niniejszym oświadczam, że zapoznałem(am) się z przepisami 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 (opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1) i zobowiązuję się do:

1) przetwarzania danych osobowych powierzonych do przetwarzania przez Izbę Gospodarczą Handlowców, Przetwórców Zbóż i Producentów Pasz tylko w zakresie niezbędnym do wykonania Umowy;
2) wykorzystywania danych osobowych wyłącznie do celów, dla których zostały zebrane;
3) dochowania najwyższej staranności w celu należytego zabezpieczenia powierzonych danych osobowych przed jakimkolwiek nieuprawnionym ujawnieniem osobom trzecim;
4) dokonywania uzupełnień, uaktualnień i/lub sprostowań danych osobowych zgłoszonych przez daną osobę na podstawie wiarygodnych dokumentów (dowód osobisty, paszport, akta stanu cywilnego, świadectwa pracy, prawo jazdy);
5) zachowania ścisłej tajemnicy odnośnie przetwarzania danych, a w szczególności danych osobowych, zarówno w okresie zatrudnienia jak i po ustaniu zatrudnienia;
6) niekopiowania danych na jakiekolwiek nośniki i wykorzystania ich na użytek własny bądź innych nieupoważnionych osób.

Imię i Nazwisko ……
Adres: ……
Data i czytelny podpis: ……

ZAŁĄCZNIK NR 4
Upoważnienie do Przetwarzania Danych Osobowych
[WZÓR]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 29 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 (opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1) („**Rozporządzenie**")
udziela się Panu/Pani*:

……

(imię i nazwisko)

upoważnienia do przetwarzania danych osobowych w rozumieniu wyżej wymienionego Rozporządzenia. Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych, których administratorem jest Izba Gospodarcza Handlowców, Przetwórców Zbóż i Producentów Pasz wyłącznie w zakresie:

Lp.		**Kategoria danych**
1.	□	Dane Osobowe pracowników i współpracowników
2.	□	Dane Osobowe byłych pracowników i współpracowników
3.	□	Dane Osobowe kandydatów do pracy
4.	□	Dane Osobowe kontrahentów
5.	□	Dane Osobowe członków Rady Izby
6.	□	Dane osobowe osób reprezentujących firmę (członka) w Izbie

Upoważnienie traci ważność z chwilą ustania stosunku pracy lub współpracy.

(Data, imię i nazwisko oraz podpis osoby reprezentującej Izbę Gospodarczą Handlowców, Przetwórców Zbóż i Producentów Pasz)	*(Data i podpis osoby upoważnionej)*

ZAŁĄCZNIK NR 4A

Upoważnienie do Przetwarzania Danych Osobowych dla pracowników podmiotów zewnętrznych [WZÓR]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 29 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 (opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1) („**Rozporządzenie**") oraz w związku z umową z dnia ……. pomiędzy Izbą Gospodarczą Handlowców, Przetwórców Zbóż i Producentów Pasz oraz ……w sprawie

……

udziela się Panu/Pani*:

……

(imię i nazwisko)

upoważnienia do przetwarzania danych osobowych w rozumieniu wyżej wymienionego Rozporządzenia. Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych Osobowych, których administratorem jest Izba Gospodarcza Handlowców, Przetwórców Zbóż i Producentów Pasz wyłącznie w zakresie:

Lp.		**Kategoria danych**
1.	□	Dane Osobowe pracowników i współpracowników
2.	□	Dane Osobowe byłych pracowników i współpracowników
3.	□	Dane Osobowe kandydatów do pracy
4.	□	Dane Osobowe klientów
5.	□	Dane Osobowe członków Rady Izby
6.	□	Dane osobowe osób reprezentujących firmę (członka) w Izbie

Upoważnienie traci ważność z chwilą wygaśnięcia umowy lub podjęcia decyzji przez Izbę Gospodarczą Handlowców, Przetwórców Zbóż i Producentów Pasz

(Data, imię i nazwisko oraz podpis osoby reprezentującej Izbę Gospodarczą Handlowców, Przetwórców Zbóż i Producentów Pasz)	*(Data i podpis osoby upoważnionej)*