POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH OBOWIĄZUJACA W INTEGROTECH sp. z o.o.

Spis treści

§ 1. Wprowadzenie

1. Polityka Bezpieczeństwa Danych Osobowych w dalszej części dokumentu zwana Polityką opracowana została w oparciu o następujące przepisy prawa:
   a. 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, zwanego w dalszej części dokumentu RODO,
   b. Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych .

2. Polityka określa zbiór zasad przetwarzania danych osobowych w INTEGROTECH sp. z o.o. oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji.

3. Celem Polityki jest wdrożenie i realizacja działań przy wykorzystaniu takich dostępnych środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo w zakresie przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem lub przetwarzaniem z naruszeniem przepisów oraz przed zmianą, uszkodzeniem lub zniszczeniem.

4. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   - poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
   - integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   - rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
   - zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania jednostki.

5. Polityka zakłada pełne zaangażowanie kierownictwa oraz wszystkich pracowników INTEGROTECH sp. z o.o. dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny papierowy, jak i w systemach informatycznych czy innych nośnikach danych.

6. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawa, stanem techniki i strukturą organizacyjną firmy oraz innymi czynnikami, które powodują, że określone zasady przestają być aktualne.

§ 2. Definicje

1. **Administrator Danych Osobowych [ADO]** – osoba decydująca o celach i środkach przetwarzania danych osobowych – PrezesZarządu.

2. **Administrator Infrastruktury Informatycznej [AII]** - osoba nadzorująca rozwój i utrzymanie infrastruktury informatycznej wykorzystywanej do przetwarzania lub magazynowania danych osobowych.

3. **Administrator Systemów Informatycznych [ASI]** - osoba nadzorująca rozwój i utrzymanie struktury systemów informatycznych wykorzystywanych do przetwarzania lub magazynowania danych osobowych.

4. **Dane osobowe** [DO]– każda informacja dotycząca osoby fizycznej, która w sposób pośredni lub bezpośredni pozwala ją zidentyfikować, w szczególności poprzez podanie jednego lub kilku specyficznych czynników ją określających.

5. **PUODO – Prezes Urzędu Ochrony Danych Osobowych .**

6. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe działanie lub zaniechanie działania, powodujące zagrożenie ezpieczeństwa danych osobowych, przetwarzanych tradycyjnie, jak również z wykorzystaniem systemów informatycznych.

7. **Osoba upoważniona** [OSU]– osoba posiadająca imienne upoważnienie wydane przez Administratora Danych Osobowych i dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

8. - **Przetwarzanie danych osobowych** [PDO]– jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

9. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych .

10. **System informatyczny** –zbiór programów wspólnie tworzących programistyczne środowisko informatyczne, w którym zachodzi przetwarzanie i magazynowanie informacji w celu przetwarzania danych, w tym danych osobowych.

11. Infrastruktura informatyczna - zbiór współpracujących lub autonomicznych urządzeń wspólnie tworzących sprzętowe środowisko informatyczne, w którym zachodzi przetwarzanie i magazynowanie informacji w celu przetwarzania danych, w tym danych

osobowych.

12. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

13. **Zbiór nieinformatyczny** – zbiór danych osobowych prowadzony w formie papierowej poza systemem informatycznym.

§ 3. Deklaracja Administratora Danych Osobowych

Administrator Danych zobowiązuje się do podjęcia odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności zapewnia, że dane osobowe są:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i nie są poddawane dalszemu przetwarzaniu niezgodnie z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
- zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność i poufność tych danych.

§ 4. Przegląd dokumentacji ochrony danych osobowych.

1. Niniejsza Polityka oraz dokumenty z nią powiązane winny być aktualizowane wraz ze zmianami prawnymi czy też zmianami faktycznymi w ramach organizacji, które mogą spowodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne.
2. Zadaniem przeglądu jest stwierdzenie, czy postanowienia normowane Polityką odpowiadają aktualnej działalności INTEGROTECH sp. z o.o. oraz stanowi prawnemu w momencie dokonywania przeglądu.
3. Fakt wystąpienia naruszeń winien skutkować zmianami Polityki i dokumentacji powiązanej.
4. Wszelkie zmiany Polityki – mające wpływ na poziom bezpieczeństwa ochrony danych osobowych – winny być zatwierdzane przez Administratora Danych Osobowych.

§ 5. Zarządzanie obszarem ochrony danych osobowych

1. Realizację zadań mających na celu zwiększenie skuteczności ochrony danych osobowch powinny zagwarantować następujące założenia:

- przeszkolenie pracowników dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych,
- przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień,
- okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
- prowadzenie cyklicznych przeglądów, aktualizacja i wdrażanie rozwiązań określonych w wyniku przeprowadzonych przeglądów,
- podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych,
- śledzenie osiągnięć w dziedzinie bezpieczeństwa fizycznego, bezpieczeństwa systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych,
- wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.

2. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie: integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
3. Administrator Danych powinien mieć pewność, że pracownicy oraz współpracownicy:
   - są odpowiednio wprowadzani w swoje obowiązki i są świadomi odpowiedzialności związanej z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych,
   - otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami służbowymi,
   - wypełniają zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy,
   - w sposób ciągły utrzymują odpowiednie umiejętności i kwalifikacje.
4. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba, przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami i rolą sprawowaną w procesie.

§ 6. Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych jest odpowiedzialny za przetwarzanie danych osobowych oraz za ich ochronę zgodnie z przepisami prawa. W tym celu zobowiązany jest do wprowadzenia do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   - określenie celów i procedur ochrony danych osobowych,
   - podział zadań i obowiązków związanych z organizacją obszaru ochrony danych osobowych.
3. Do obowiązków Administratora Danych należy:
   a. zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych,
   b. zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem
   c. przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych,
   d. nadawanie pracownikom upoważnień do przetwarzania danych osobowych,
   e. zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe oraz środków niezbędnych do zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych przetwarzanych w systemach informatycznych,
   f. zapewnienie płynnej realizacji przeglądów zapewnianej ochrony danych osobowych na podstawie przepisów prawa.

§ 7. Odpowiedzialność Administratora Systemów Informatycznych

1. Funkcję Administratora Systemów Informatycznych pełni pracownik wyznaczony przez Administratora Danych Osobowych.

2. Do obowiązków Administratora Systemów Informatycznych należy:
   a. zapewnienie wdrożenia systemów przetwarzania danych osobowych,
   b. nadzór nad zapewnianiem ciągłości działania systemu informatycznego,
   c. reagowanie na przypadki naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,
   d. przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych magazynowanych lub przetwarzanych w Systemie Informatycznym,
   e. zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą, RODO oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym,
   f. administrację oprogramowania systemu zabezpieczającego dane osobowe przed nieupoważnionym dostępem,
   g. przyznawanie za zgodą Administratora Danych Osobowych, ściśle określonych praw dostępu do danych osobowych w danym systemie,
   h. świadczenie pomocy technicznej użytkownikom oprogramowania PDO,
   i. diagnozowanie i usuwanie awarii systemu informatycznego służącego PDO,
   j. nadzór nad wdrożeniem i zarządzanie systemami Informatycznymi (przeglądanie,

nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe,

k. umożliwienie przeprowadzenia kontroli systemu informatycznego przez Prezesa Urzędu Ochrony Danych Osobowych .

§ 8. Odpowiedzialność Administratora Infrastruktury Informatycznej

1. Funkcję Administratora Infrastruktury Informatycznej [AII] pełni pracownik wyznaczony przez Administratora Danych Osobowych.

1. Do obowiązków Administratora Infrastruktury Informatycznej należy;
   1.1. nadzór nad zapewnieniem właściwej infrastruktury dla celów związanych z przetwarzaniem danych osobowych,
   1.2. nadzór nad zapewnianiem ciągłości działania infrastruktury informatycznej,
   1.3. reagowanie na przypadki naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,
   1.4. przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych,
   1.5. zapewnienie zgodności wszystkich wdrażanych elementów infrastruktury przetwarzania danych osobowych z Ustawą, RODO oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym,
   1.6. zapewnienie poprawnej instalacji oraz konfiguracji, eksploatacji i wycofania z eksploatacji: oprogramowania, sprzętu stacjonarnego, mobilnego, infrastruktury sieci teleinformatycznej i serwerów używanych do przetwarzania danych osobowych [PDO],
   1.7. nadzór nad konfiguracją i administracją oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem,
   1.8. nadzór nad okresową weryfikacją infrastruktury używanej do PDO pod kątem obecności szkodliwego oprogramowania,
   1.9. zapewnienie pomocy technicznej użytkownikom oprogramowania a także serwisu sprzętu komputerowego będącego na stanie przedsiębiorstwa, służącego do przetwarzania danych osobowych,
   1.10. diagnozowanie i usuwanie awarii sprzętu komputerowego,
   1.11. nadzór nad procesem wykonywania kopii bezpieczeństwa i zarządzanie kopiami bezpieczeństwa oprogramowania systemowego infrastruktury służącej PDO,

§ 9. Odpowiedzialność pracowników i użytkowników systemu

1. W celu zapewnienia wysokiego poziomu bezpieczeństwa danych osobowych konieczne jest zaangażowanie każdego pracownika i użytkownika w proces ochrony danych osobowych.
2. Pracownicy oraz użytkownicy odpowiedzialni są za bezpieczeństwo danych, do których mają dostęp zgodnie z przyznanymi upoważnieniami.
3. Do obowiązków pracowników oraz użytkowników należy:

a. informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach Ustawy,
b. postępowanie zgodnie z przyjętą Polityką,
c. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
d. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
e. ścisłe przestrzeganie zakresu nadanego upoważnienia do przetwarzania danych osobowych,
f. przestrzeganie procedur związanych z otwieraniem i zamykaniem pomieszczeń, w których przetwarzane są dane osobowe, w tym również zapobieganie sytuacjom, w których dostęp do danych osobowych mogą mieć osoby nieupoważnione,

§ 10 Sankcje prawne za naruszenie zasad ochrony danych osobowych.

1. W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej.
2. Naruszenie obowiązków przez pracownika może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy lub odpowiedzialności cywilnej.
3. Naruszenie obowiązków przez użytkownika, nie będącego pracownikiem może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie umowy cywilnoprawnej łączącej Administratora oraz użytkownika i może skutkować odpowiedzialnością odszkodowawczą względem niego.
4. Naruszenie zasad ochrony danych osobowych a także sposobu ich zabezpieczania, może skutkować postawieniem pracownikowi lub użytkownikowi, zarzutu popełnienia jednego z przestępstw określonych w art. 266 Kodeksu Karnego.

§ 11. Wymiana informacji dotyczących danych osobowych

1. W celu ochrony danych pracownicy oraz użytkownicy podczas przetwarzania daych osobowych winni uwzględniać następujące zasady:
   a. wykorzystywać techniki kryptograficzne do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi,

b. chronić dane osobowe przed przechwyceniem, kopiowaniem, modyfikacją lub zniszczeniem,
c. wykorzystywać możliwości techniczne wykorzystywanych systemów komunikacji do zabezpieczenia treści i ograniczania ewentualnego niekontrolowanego przekazywania wiadomości za pomocą stosowanych środków komunikacji,
d. respektować zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, do których mogą mieć dostęp osoby nieupoważnione,
e. zachowywać szczególną ostrożności w trakcie rozmów telefonicznych, w tym w szczególności upewnić się, że rozmówcą jest osoba upoważnioną do uzyskania określonych danych osobowych, jak również nie pozostawiać wiadomości zawierających dane osobowe na poczcie głosowej odbiorcy,
f. okresowo, lub najpóźniej w dniu wycofania z eksploatacji, kasować wbudowaną pamięć podręczną faksów i kopiarek.
g. elektroniczne nośniki danych o ile są wykorzystywane także okazjonalnie do magazynowania lub przetwarzania danych osobowych (dyski zewnętrzne, pendrivy, dyski wbudowane w komputery i laptopy) winny być zaszyfrowane i regularnie skanowane przy użyciu zatwierdzonych w Integrotech sp. z o.o. narzędzi informatycznych, a po wycofaniu z eksploatacji poddane kasowaniu lub utylizacji przy użyciu adekwatnie do zadania certyfikowanych narzędzi informatycznych lub przez certyfikowany zgodnie z wymaganiami ustawy podmiot gospodarczy,

§ 12. Identyfikacja obszarów bezpiecznych

1. Dane osobowe w INTEGROTECH sp. z o.o. mogą być przetwarzane wyłącznie w miejscach zapewniających adekwatny do realizowanej funkcji poziom bezpieczeństwa przetwarzania danych osobowych, który jest oceniany każdorazowo przez Osobę Upoważnioną przed podjęciem czynności związanych z przetwarzaniem.
2. Do miejsc/lokalizacji przetwarzania danych osobowych zalicza się:
   - pomieszczenia techniczne i biurowe, w których znajdują się stacje robocze,
   - pomieszczenia lub miejsca , w których przechowywane są dokumenty oraz wydruki z systemu informatycznego,
   - pomieszczenia lub miejsca, w których znajdują się zbiory nieinformatyczne,
   - pomieszczenia lub miejsca w których znajdują się sprawne oraz uszkodzone elektroniczne nośniki informacji oraz kopie zapasowe danych osobowych,

   w czasie gdy następują w nich czynności przetwarzania lub magazynowania danych osobowych.
3. Na czas przetwarzania danych osobowych budynki lub pomieszczenia, w których są one przetwarzane winny być zamykane na czas nieobecności osób upoważnionych do przetwarzania danych osobowych w sposób ograniczający możliwość przypadkowego dostępu do nich osobom nieupoważnionym.

4. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których przetwarzane są dane osobowe należy:
- określić granice obszaru przetwarzania danych osobowych oraz jego umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru,
- stosować systemy zapobiegania nieautoryzowanym naruszeniom obszaru i wykrywania włamań do obszaru.

5. Obszary bezpieczne winny być odpowiednio zabezpieczone przed skutkami pożaru (ochrona p.poż.).
6. Ochrona obszarów bezpiecznych winna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko osoby upoważnione mogą uzyskać do nich legalny dostęp. W tym celu należy zapewnić:
   - nadzór pobytu osób nie będących osobami upoważnionymi w obszarach bezpiecznych,
   - kontrolę i ograniczenie dostępu do obszarów, w których przetwarzane są dane osobowe, tylko do osób uprawnionych,
   - przegląd praw dostępu do obszarów bezpiecznych.
7. Nośniki elektroniczne zawierające dane osobowe winny być ewidencjonowane i bezpiecznie przechowywane w obszarach magazynowania lub przetwarzania danych osobowych.

§ 13. Środki ochrony danych osobowych

1. Administrator Danych Osobowych zobowiązany jest zapewnić zastosowanie środków technicznych oraz organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych.
2. Środki ochrony obejmują:
   - środki fizyczne,
   - środki osobowe,
   - środki techniczne.
3. Środki ochrony fizycznej obejmują:
   -nadzorowanie pobytu osób nieposiadających upoważnienia do przetwarzania danych osobowych w obszarach bezpiecznych przez osoby upoważnione,
   -lokalizację miejsc przetwarzania danych osobowych,
   - przechowywanie zbiorów danych osobowych w miejscach odpowiednio zabezpieczonych,
   - wdrożenie procedur uzyskiwania narzędzi legalnego dostępu do tych miejsc.
4. Środki ochrony osobowej obejmują:

- dopuszczenie do danych osobowych wyłącznie osób posiadających imienne upoważnienie do przetwarzania danych osobowych wydane za zgodą Administratora Danych Osobowych,
- przeszkolenie użytkowników z zakresu ochrony danych osobowych,
- zgromadzenie stosownych oświadczeń o zachowaniu w poufności danych osobowych.

5. Środki ochrony technicznej obejmują:
   - mechanizmy i procedury kontroli dostępu do systemów i zasobów,
   - informatyczne narzędzia ochronne,
   - procedury tworzenia kopii zapasowych,
   - ewidencję przenośnych nośników informacji z danymi osobowymi,
   - procedury postępowania z przenośnymi komputerami, dyskami i nośnikami informacji, na których mogą być gromadzone dane osobowe.

§ 14. Zasady ochrony zbiorów nieinformatycznych

1. Zbiory nieinformatyczne winny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki zawierające dane osobowe należy przechowywać w odpowiednio zabezpieczonych miejscach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nieużytkowania dokumenty i wydruki zawierające dane osobowe winny być zamykane w szafkach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane winny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§ 15. Dopuszczenie do przetwarzania danych osobowych / ewidencja osób upoważnionych

1. Pracownicy i użytkownicy mają prawo do przetwarzania danych osobowych wyłącznie po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych, wystawionego przez Administratora Systemów Informatycznych za zgodą Administratora Danych Osobowych.
2. W tym celu Administrator Systemów Informatycznych przed dopuszczeniem pracownika lub użytkownika do pracy przy przetwarzaniu danych osobowych:
   - zapoznaje go z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w jednostce,
   - wystawia mu formalne upoważnienie do przetwarzania danych osobowych, zgodnie ze wzorem upoważnienia stanowiącym załącznik nr 1 do niniejszej Polityki,

- przyjmuje od niego podpisane oświadczenie o zachowaniu w poufności danych osobowych i sposobów ich zabezpieczenia, zgodnie ze wzorem oświadczenia stanowiącym załącznik nr 2 do niniejszej Polityki,
- upoważnienia i oświadczenia, o którym mowa powyżej przechowuje się w aktach osobowych pracownika, a w przypadku innych osób, wraz z umową zawartą pomiędzy osobą upoważnioną a Administratorem Danych Osobowych.

3. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzana danych osobowych prowadzona jest przez Administratora Danych Osobowych i powinna zawierać:
   - imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych,
   - zakres upoważnienia do przetwarzania danych osobowych,
   - identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych,
   - datę nadania i odebrania uprawnień.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych winna być przechowywana w szafie zamykanej, do której dostęp ma Administrator Danych Osobowych oraz Administrator Systemów Informatycznych.
5. Wzór karty z ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.

§ 16. Opis struktury zbiorów danych osobowych

1. Dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, wydruków, ksiąg i wykazów.
2. Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych musi być zgodna z przepisami prawa.
3. Administrator Danych Osobowych prowadzi ewidencję stosowanych systemów i programów (w tym licencji oprogramowania) zastosowanych do przetwarzania danych osobowych.
4. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
5. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu".
6. Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu" i „do zapisu", tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących.
7. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. płyta CD, DVD, dysk wymienny, PenDrive itp.)

lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/ importu danych za pomocą teletransmisji (np. poprzez szyfrowaną sieć teleinformatyczną).

§ 17. Udostępnienie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub za zgodą osoby, której dane osobowe dotyczą.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych, może nastąpić wyłącznie za zgodą Administratora Danych Osobowych. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie w celu, dla którego zostały pozyskane oraz udostępnione.
4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Administrator Danych Osobowych.
6. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowana i podpisywana przez Administratora Danych Osobowych.

§ 18. Powierzanie danych osobowych współpracującym podmiotom zewnętrznym

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Integrotech sp. z o.o. mają dostęp do przetwarzanych przez spółkę danych osobowych .

2. Powierzenie, o którym mowa powyżej, może mieć miejsce wyłącznie na podstawie stosownej pisemnej klauzuli powierzenia zawartej w umowach celowych dotyczących powierzenia DO lub innych regulujących wzajemne relacje, lub warunki realizacji przedmiotu umowy, które są zawierane pomiędzy stronami z udziałem Integrotech sp. z o.o., a podmiotem, któremu zostanie powierzone przetwarzanie danych osobowych administrowanych przez Spółkę.

§ 19. Prowadzenie przeglądów

1. Przeglądy są dokonywane przez Administratora Systemów Informatycznych:
   - cyklicznie, według planu przeglądów przygotowywanego co roku przez Administratora Danych Osobowych,
   - - na zlecenie Administratora Danych, w sytuacji powzięcia informacji o naruszeniu procedur ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;

- na każde żądanie PUODO.

2. Przegląd jest przeprowadzany w trybach określonych w przepisach prawa, tj. w trybie:
   - sprawdzenia planowego
   - sprawdzenia doraźnego
   - sprawdzenia dla PUODO w przypadku zwrócenia się o dokonanie sprawdzenia przez PUODO.

3. Plan przeglądów, o którym mowa w ust. 1 powyżej, określa przedmiot, zakres czynności oraz planowany termin przeprowadzenia sprawdzenia.
4. Administrator w planie przeglądów uwzględnia w szczególności potrzebę inwentaryzacji zbiorów danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych.
5. Administrator Danych Osobowych w przypadku zlecenia dokonania przeglądu w związku z powzięciem informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzenia wystąpienia takiego naruszenia określa:
   - zakres czynności, które winny być podjęte w toku sprawdzenia,
   - sposób i zakres dokumentowania czynności niezbędnych do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania raportu.

6. W toku przeglądu Administrator Danych Osobowych może podejmować następujące czynności:
   - zbieranie ustnych i pisemnych wyjaśnień od osób objętych sprawdzeniem,
   - przeprowadzanie oględzin miejsc przetwarzania danych osobowych,
   - analizowanie dokumentów dotyczących przetwarzania danych osobowych.
7. Administrator Danych Osobowych może dokumentować czynności poprzez:
   - utrwalenie danych na nośniku,
   - sporządzenie notatki służbowej,
   - sporządzenie protokołu odebrania ustnych wyjaśnień,
   - sporządzenie protokołu z oględzin,
   - sporządzenie kopii otrzymanego dokumentu,
   - sporządzenie kopii obrazu wyświetlanego na ekranie,
   - sporządzenie kopii rejestrów systemu informatycznego służącego do przetwarzania danych osobowych.
8. Przegląd zakończony jest sprawozdaniem:
   - ze sprawdzenia planowego – w terminie określonym w planie przeglądów, nie później niż w terminie 30 dni od zakończenia sprawdzenia,
   - ze sprawdzenia na zlecenie Administratora – niezwłocznie po zakończeniu sprawdzenia, w formie raportu, z uwzględnieniem danych wskazanych w art. 33 RODO,
   - ze sprawdzenia, o którego dokonanie zwrócił się PUODO – w terminie wskazanym przez PUODO .

§ 21. Postanowienia końcowe

Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą wyciągnięcia konsekwencji służbowych zgodnych z rodzajem nawiązanego stosunku pracy wobec osoby która dopuściła się naruszenia.

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz RODO.

Łódź, 14 maja 2018 r.

Integrotech sp. z o.o.
mgr inż. Piotr Łuczak
PREZES ZARZĄDU

Załączniki

Integralną część Polityki stanowią załączniki:

Załącznik nr 1 - Upoważnienie do przetwarzania danych osobowych

Załącznik nr 2 - Oświadczenie osoby uprawnionej do przetwarzania danych osobowych

Załącznik nr 3 - Ewidencja osób upoważnionych do przetwarzania danych

Załącznik nr 4 - Wykaz zbiorów i systemów służących do ich przetwarzania

Załącznik nr 1
Do Polityki Bezpieczeństwa Danych

Łódź, dn..... r.

UPOWAŻNIENIE nr .....
do przetwarzania danych osobowych

1. Niniejszym z dniem ..... r. nadaję Panu ..... zatrudnionemu przez INTEGROTECH sp. z o.o. – administratora danych osobowych, na stanowisku ....., upoważnienie do przetwarzania danych osobowych gromadzonych w:
   a. .....
   b. .....
2. Upoważnienie dotyczy .....
3. Jest Pan upoważniony do przetwarzania danych osobowych wyłącznie w celu wynikającym z Pana zadań służbowych oraz poleceń przełożonego.
4. Upoważnienie wygasa z chwilą jego cofnięcia, rozwiązania umowy o pracę lub zmiany stanowiska pracy.
5. Jednocześnie zobowiązuję Pana do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia.

Podstawa prawna:
Art. 37 i 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.)

Adnotacja o cofnięciu upoważnienia (data cofnięcia, przyczyna)
.....
.....

....
miejscowość, data Administrator Bezpieczeństwa Danych

Załącznik nr 2

Do Polityki Bezpieczeństwa Danych

Oświadczenie

Ja niżej podpisany oświadczam, że zostałem przeszkolony, zapoznałem się i będę przestrzegać obowiązków związanych z ochroną danych osobowych, które wynikają z 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, przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych z późniejszymi zmianami, aktów wykonawczych wydanych na ich podstawie oraz dokumentów przyjętych przez INTEGROTECH sp. z o.o. w związku z przetwarzaniem danych osobowych, a w szczególności:

- Polityką bezpieczeństwa przetwarzania danych osobowych w INTEGROTECH sp. z o.o.;
- Instrukcją zarządzania systemem informatycznym w INTEGROTECH sp. z o.o..

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie zatrudnienia (niezależnie od formy prawnej zatrudnienia), jak również po ustaniu zatrudnienia.

Jednocześnie jestem świadomy odpowiedzialności za niedopełnienie obowiązków wynikających z przepisów prawa, jaka ciąży na mnie na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych i Rozporządzenia.

.....

Data, czytelny podpis (imię i nazwisko)

Przyjąłem do wiadomości

.....

Administrator Danych Osobowych

Załacznik nr 3

Do Polityki Bezpieczeństwa Danych

Ewidencja osób upoważnionych do przetwarzania danych osobowych w INTEGROTECH sp. z o.o.

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia		Login / Identyfikator	Nr upoważnienia
				Stanowisko służbowe	Dostęp do systemów / zbiorów		
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							