POLITYKA OCHRONY
DANYCH OSOBOWYCH

Administrator danych osobowych:

Firma:	ABIMULANA SYLWESTER TKOCZ
Adres siedziby:	ul. Wrocławska 1B, 55-050 Strzegomiany
NIP:	8961551691
REGON:	364560837
Forma prawna przedsiębiorstwa *(np. spółka z o.o., spółka jawna, jednoosobowa działalność gospodarcza)*	jednoosobowa działalność gospodarcza

Spis treści:

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Polityka ochrony danych osobowych zwana dalej „Polityką", określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, sposób przepływu danych pomiędzy poszczególnymi systemami, zawiera wykaz budynków oraz pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu, a także ocenę ryzyka naruszenia danych osobowych.
2. Polityka została opracowana zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

§ 2

Ilekroć w Polityce jest mowa o:

1. **danych osobowych** – oznacza to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
2. **zbiorze danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten

jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

3. **przetwarzaniu danych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

4. **procesie przetwarzania danych osobowych** – oznacza ciąg następujących po sobie czynności począwszy od zebrania danych osobowych, aż do ich usunięcia,

5. **administrator** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

6. **podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,

7. **użytkownikach –** oznaczona to osoby fizyczne przetwarzające dane osobowe w imieniu administratora, współpracujące z administratorem w ramach prowadzonej działalności, niezależnie od podstawy prawnej współpracy

8. **naruszenie danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

9. **strona trzecia –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,

10. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

11. **kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe.

12. **pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych Osobowych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem własnego sprzętu komputerowego oraz gromadzone w kartotekach,

13. **przedsiębiorca** – oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.

§ 3

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez:
    1. zabezpieczenia fizyczne,
    2. procedury organizacyjne,
    3. oprogramowanie systemowe oraz
    4. podmioty przetwarzające.
2. Zastosowane zabezpieczenia gwarantują:
    2.1. **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
    2.2. **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

2.3. **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

2.4. **integralność systemu** - rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji,

2.5. **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 4

1. Realizację zamierzeń określonych w § 3 ust. 2 powinny zagwarantować następujące założenia:
   1.1. wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
   1.2. przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
   1.3. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).

§ 5

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1.1. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
   1.2. wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione *(np. zmian zawartości danych, utrat całości lub części danych),*
   1.3. naruszenie lub próby naruszenia integralności systemu,
   1.4. zmianę lub utratę danych zapisanych na kopiach zapasowych,
   1.5. naruszenie lub próby naruszenia poufności danych lub ich części,
   1.6. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   1.7. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,

1.8. zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach,

1.9. inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.

2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II

Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6

1. Fizyczna ochrona danych osobowych przetwarzanych za pośrednictwem:
   1.1. kartotek – ochrona realizowana jest poprzez ich zabezpieczenie w miejscu ich przechowywania w sposób uniemożliwiający dostęp osoby trzecich.
   1.2. urządzeń elektronicznych – ochrona realizowana jest poprzez wyznaczenia pomieszczeń w których znajdują się urządzenia elektroniczne oraz ich zabezpieczenie w sposób uniemożliwiający dostęp osób trzecich.
2. Procedury organizacyjne wdrożone w celu zabezpieczenia ochrony danych osobowych:
   2.1. współpraca z podmiotami przetwarzającymi jest możliwa wyłącznie po wcześniejszym zabezpieczaniu prawnym tj.
      2.1.1. z każdym przedsiębiorcą rozpoczynającym współpracę okresową sporządzona jest umowa powierzenia danych osobowych, z której wynika zakres powierzonych danych osobowych.
      2.1.2. każda osoba przed dopuszczeniem do dostępu do danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
3. Oprogramowanie systemowe służące do zabezpieczenia ochrony danych osobowych pochodzi wyłącznie z legalnych źródeł dystrybucji i jest na bieżąco aktualizowane.

ROZDZIAŁ III

Przetwarzanie danych osobowych

§ 7

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz kartotek odbywa się wyłącznie na obszarze wyznaczonym przez administratora.
2. Przetwarzanie danych osobowych za pomoc urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą administratora.
3. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych.

4. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.
5. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.
6. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

§ 8

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko upoważnieni użytkownicy.
2. Upoważnienie nadaje i odwołuje administrator.
3. Upoważnienie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano upoważnienie, drugi – dla administratora. Wzór upoważnienia do przetwarzania danych osobowych określa **załącznik nr 1 do Polityki**.
4. Administrator prowadzi ewidencję osób przetwarzających dane w przedsiębiorstwie posiadających upoważnienie. Wzór ewidencji określa **załącznik nr 2 do Polityki**.
5. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności użytkownika wyznaczonego w tym celu przez administratora.

§ 9

1. Wykaz procesów przetwarzania danych osobowych oraz kategorii danych osobowych przetwarzanych w ramach tychże procesów określa **załącznik Nr 3 do Polityki.**
2. Ryzyko związane z przetwarzaniem danych osobowych określa **załącznik Nr 3 do Polityki,** z którego wynika stopień zagrożenia przetwarzania danych osobowych oraz środki wdrożone w celu zabezpieczenia danych.

3. Wykaz podmiotów, którym administrator przekazuje dane osobowe na podstawie umów powierzenia przetwarzania danych osobowych zawiera **załącznik Nr 4 do Polityki.**

ROZDZIAŁ IV

Instrukcja zarządzania systemem informatycznym

§ 10

1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika (login) i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem.

2. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.

3. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora.

4. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

5. Administrator jest zobowiązany do wprowadzenia częstotliwości zmiany haseł przez użytkowników.

§ 11

1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić administratora.

2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

3. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

4. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyty CD, pendrive i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

§ 12

1. Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik.
2. Kopie zapasowe powinny być kontrolowane przez administratora, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
3. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
4. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.
5. Za realizację żądania osoby, której dane dotyczą do usunięcia jej danych z danych administratora odpowiada administrator lub użytkownik przez niego wyznaczony.
6. Za realizację przeniesienia danych osobowych odpowiada administrator lub użytkownik przez niego wyznaczony.

§ 13

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest:

1. oprogramowanie antywirusowe,
2. zapory ogniowe,
3. szyfrowanie,
4. oraz okresowe szkolenie użytkowników za zakresu najnowszych zagrożeń.

2. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe oraz zapora ogniowa. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

§ 14

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, przez firmy zewnętrzne na podstawie zawartych umów.
2. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora.
3. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator.

ROZDZIAŁ V

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 15

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie administratora lub upoważnioną przez niego osobę.
3. Postanowienia ust. 2 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w kartotekach.

§ 16

1. Administrator o incydencie zawiadamia organ nadzorczy. Informacja powinna zostać przekazana niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.
2. Administrator prowadzi rejestr naruszeń danych osobowych, który stanowi **załącznik nr 5** do niniejszej Polityki.
3. Administrator lub osoba przez niego upoważniona podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   3.1. w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
   3.2. o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 17

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od administratora lub osoby przez niego upoważnionej.

2. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia administratora lub upoważnioną przez niego osobę, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym administrator lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

ROZDZIAŁ V
Postanowienia końcowe

§ 18

1. Polityka jest dokumentem wewnętrznym, zawiera dane, których ujawnienie mogłoby spowodować utratę danych chronionych w związku z czym nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej w formie pisemnej, przetwarzanie danych osobowych w przedsiębiorstwie. Podmiot ten, może przetwarzać dane wyłącznie w zakresie i celu wskazanym w umowie.

§ 19

1. Administrator jest zobowiązany zapoznać z treścią Polityki każdego użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami związanymi z ochroną danych osobowych oraz wykazać się certyfikatem ukończonego szkolenia w zakresie ochrony danych osobowych.

§ 20

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydane na jej podstawie akty wykonawcze.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.