POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
SKLEPU INTERNETOWEGO
WWW.KOMINKINABIOPALIWO.PL

„MILA”
TOMASZ MILA
UL. ALEKSANDROWSKA 179
91-229 ŁÓDŹ

_____	_____	_____
pieczęć firmowa	podpis administratora danych osobowych	data

Wstęp

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Z 2014 r., poz. 1182 ze zm.), art. 36 w/w ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, administrator danych osobowych zobowiązany jest do zapewnienia ochrony przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jakość zapewnianej ochrony powinna być odpowiednia do zagrożeń oraz kategorii danych nią objętych. Ponadto zgodnie z art. 38 ustawy administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Biorąc pod uwagę te konstytucyjne i ustawowe obowiązki wprowadzamy następujący zestaw procedur i rozwiązań, stanowiący Politykę bezpieczeństwa przetwarzania danych osobowych niniejszego Sklepu internetowego.

Rozdział 1
Postanowienia ogólne

§ 1

Ilekroć w Polityce bezpieczeństwa jest mowa o:

1. **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.);
2. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
3. **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
4. **przetwarzaniu danych** – rozumie się przez to 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;
5. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8. **administratorze danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
9. **zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;

10. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
11. **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
12. **obszarze przetwarzania danych** – należy przez to rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
13. **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
14. **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
15. **opisie przepływu danych** – należy przez to rozumieć opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi;
16. **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Rozdział 2
Administrator danych

§ 2

Administrator danych jest zobowiązany w szczególności do:

1. opracowania i wdrożenia Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe;
2. wydawania i anulowania upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać (załącznik nr 1);
3. prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych (załącznik nr 2);
4. prowadzenia wykazu obszarów przetwarzania (załącznik nr 3);
5. prowadzenia wykazu zbiorów danych osobowych (załącznik nr 4);
6. prowadzenie opisu struktury zbiorów (załącznik nr 5);
7. prowadzenia opisu sposobu przepływu danych (załącznik nr 6);
8. zgłaszania Generalnemu Inspektorowi Danych Osobowych (GIODO) zbiorów danych podlegających rejestracji.

Rozdział 3
Środki techniczne i organizacyjne

§ 3

W celu ochrony danych spełniono wymogi, o których mowa w art. 36–39 ustawy:

a) administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji;
b) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych
c) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
d) została opracowana i wdrożona Polityka bezpieczeństwa;
e) została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym.

§ 4

W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
b) pomieszczenia, w których przetwarzane są zbiory danych osobowych, wyposażone są w system alarmowy przeciwwłamaniowy,
c) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych,
d) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej,
e) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej,
f) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy,
g) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 5

W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
b) zastosowano środki uniemożliwiające wykonanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,
c) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
d) użyto systemu Firewall do ochrony dostępu do sieci komputerowej.

§ 6

W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
b) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych,
c) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,
d) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 7

W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
b) osoby zatrudnione przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie stosowanych zabezpieczeń systemu informatycznego;

c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

.

Rozdział 4
Postanowienia końcowe

§ 8

Wszelkie zasady opisane w Polityce bezpieczeństwa są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 9

Administrator danych może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych. W przypadkach, o których mowa powyżej, odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

§ 10

Polityka bezpieczeństwa obowiązuje od dnia jej zatwierdzenia przez administratora danych.

Załącznik nr 1

UPOWAŻNIENIE
do przetwarzania danych osobowych
w systemie informatycznym lub w zbiorze w wersji papierowej

Z dniem ..... upoważniam Panią/Pana .....
(*należy podać imię i nazwisko osoby upoważnionej*)

a) **do obsługi systemu informatycznego w** .....
(*należy podać nazwę administratora danych*)

w zakresie zgodnym z przydzielonymi uprawnieniami dostępowymi do systemów informatycznych;

b) **do obsługi zbiorów danych** .....
(*należy podać nazwę administratora danych*)

w wersji papierowej w zakresie zgodnym z zakresem obowiązków służbowych lub zobowiązań umownych.

Zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki bezpieczeństwa" oraz „Instrukcji zarządzania".

Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania, rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innego stosunku prawnego.

....
miejscowość, data *podpis w imieniu administratora danych*

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez administratora danych „Polityką bezpieczeństwa" oraz „Instrukcją zarządzania".
Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zobowiązań umownych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych w celach pozasłużbowych i pozaumownych o ile nie są one jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych lub zobowiązań umownych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od administratora danych osobowych,

- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych,
- korzystania z urządzeń przenośnych zgodnie z dokumentacją ochrony danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez administratora danych osobowych za ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych w rozumieniu przepisów prawa lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych.

.....

podpis osoby upoważnionej

Załącznik nr 2

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	**Nazwisko i Imię użytkownika**	**Identyfikator w systemie informatycznym**	**Wersja papierowa**	**Wersja elektroniczna**	**Data nadania upoważnienia**	**Data odebrania upoważnienia**	**Lokalizacja** *podać stanowisko lub miejsce pracy*
1.			Tak / Nie	Tak / Nie			
2.			Tak / Nie	Tak / Nie			
3.							
4.							

Dane aktualne na dzień: .....

Podpis w imieniu administratora danych: .....

Załącznik nr 3

WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Lokalizacja	Środki ochrony fizycznej danych	Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Środki ochrony w ramach narzędzi programowych i baz danych	Środki organizacyjne
1.	*91-229 Łódź* *ul. Aleksandrowska 179*	*DZ, SA, SM, KP, KZP, PPOŻ, NIS*	*IH, AUT, ANW, FW*	*PIH, PZH, WYG, BLOK,*	*OZ, SZ, OP, PE*
2.					
3.					

Legenda:

Skróty oznaczenia środków ochrony fizycznej danych:

DZ – drzwi zwykłe (niewzmacniane, nieprzeciwpożarowe)

DO – drzwi o podwyższonej odporności ogniowej >= 30 min.

DW – drzwi o podwyższonej odporności na włamanie – drzwi klasy C

KR – okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej

SA – system alarmowy przeciwwłamaniowy

SK – system kontroli dostępu

SM – system monitoringu z zastosowaniem kamer przemysłowych

SO – obszar nadzorowany przez służbę ochrony

SC – obszar nadzorowany przez służbę ochrony (całodobowo)

ZS – zamknięta niemetalowa szafa

ZM – zamknięta metalowa szafa

KP – zamknięty sejf lub kasa pancerna
KZS – kopia zapasowa przechowywana w zamkniętej niemetalowej szafie
KZM – kopia zapasowa przechowywana w zamkniętej metalowej szafie
KZP – kopia zapasowa przechowywana w zamkniętym sejfie lub kasie pancernej
KT – dane przechowywane w kancelarii tajnej
PPOŻ – system przeciwpożarowy i/lub wolno stojąca gaśnica
NIS – niszczarki do dokumentów

Skróty oznaczenia środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej:
SL – komputery połączone z lokalną siecią komputerową
UPS – zastosowano UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną
BIOS – zastosowano hasło BIOS
IH – zastosowano identyfikator użytkownika oraz hasło
TOK – zastosowano karty procesorowe oraz kod PIN lub token
BIO – zastosowano uwierzytelnienie z wykorzystaniem technologii biometrycznej
AUT – zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii
HZ – zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł
RD – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych
KRT – zastosowano środki kryptograficznej ochrony danych w teletransmisji
UT – zastosowano mechanizm uwierzytelnienia przy dostępie do środków teletransmisji
CALL – zastosowano procedurę oddzwonienia (callback) przy transmisji za pośrednictwem modemu
MD – zastosowano macierz dyskową
ANW – zastosowano program antywirusowy
FW – zastosowano system Firewall przy dostępie do sieci komputerowej
IDS – zastosowano system IDS/IPS

Skróty oznaczenia środków ochrony w ramach narzędzi programowych i baz danych:
REJ – zastosowano rejestrację zmian wykonywanych na poszczególnych elementach zbioru
DOS – określono prawa dostępu do wskazanego zakresu danych
PIH – zastosowano identyfikator użytkownika oraz hasła

PTOK – zastosowano karty procesorowe oraz kod PIN lub token
PBIO – zastosowano technologię biometryczną
PRD – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych
PZH – zastosowano okresową zmianę haseł dostępu
PKRY – zastosowano kryptograficzne środki ochrony danych
WYG – zainstalowano wygaszacze ekranów
BLOK – zastosowano automatyczną blokadę dostępu w przypadku dłuższej nieaktywności pracy użytkownika

Skróty oznaczenia środków organizacyjnych:
OZ – osoby upoważnione zostały zaznajomione z przepisami o ochronie danych
SZ – osoby upoważnione zostały przeszkolone z zabezpieczeń systemu informatycznego
OP – osoby upoważnione zostały zobowiązane do zachowania danych w poufności
PE – zastosowano politykę czystego ekranu
KZ – kopia zapasowa danych jest przechowywana w innym pomieszczeniu niż oryginał

Dane aktualne na dzień: ..... Podpis w imieniu administratora danych: .....

Załącznik nr 4

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Lp.	Nazwa zbioru danych	Program przetwarzający	Rejestracja w GIODO	Lokalizacja	Podstawa prawna przetwarzania danych w zbiorze
1.	*WWW.KOMINKINABIOPALIWO.PL - SKLEP INTERNETOWY*	*MAGNETO, ALLEGRO, INFAKT, PAYU*	*Tak*	*91-229 Łódź ul. Aleksandrowska 179*	*Zgoda osoby której dane dotyczą; art. 23 ust. 1 pkt ustawy o ochronie danych osobowych; art. 23 ust. 1 pkt. 5 ustawy o ochronie danych osobowych*
2.	*WWW.KOMINKINABIOPALIWO.PL - NEWSLETTER*	*PROGRAM DO WYSYŁKII WIADOMOŚCI E-MAIL*	*Tak*	*91-229 Łódź ul. Aleksandrowska 179*	*Zgoda osoby której dane dotyczą*

Dane aktualne na dzień: .....

Podpis w imieniu administratora danych: .....

Załącznik nr 5

OPIS STRUKTURY ZBIORÓW

Nazwa zbioru danych	Wersja papierowa	System informatyczny	Zawartość pól informacyjnych i powiązania pomiędzy nimi
WWW.KOMINKINABIOPALIWO.PL – SKLEP INTERNETOWY	Tak	Tak	dane adresowe klienta: [**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nazwa i siedizba firmy, nuemr identyfikacji podatkowej (NIP), adres e-mail, telefon] + zamówienia klienta: [**identyfikator zamówienia**, ilość towaru, wartość zamówienia, data zamówienia, data odbioru] + sprzedawane towary: [**identyfikator towaru**, numer katalogowy, nazwa towaru, nazwa producenta]
WWW.KOMINKINABIOPALIWO.PL - NEWSLETTER	Nie	Tak	dane adresowe klienta: [adres e-mail]

Dane aktualne na dzień: ..... Podpis w imieniu administratora danych: .....

Załącznik nr 6

OPIS SPOSOBU PRZEPŁYWU DANYCH

System (Moduł) A	System (Moduł) B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
MAGNETO	ALLEGRO	JEDNOKIERUNKOWO	MANUALNIE
MAGNET	INFAKT	JEDNOKIERUNKOWO	MANUALNIE
ALEGRO	PAYU	DWUKIERUNKOWO	AUTOMATYCZNIE

Dane aktualne na dzień: .....

Podpis w imieniu administratora danych……