POLITYKA BEZPIECZEŃSTWA INFORMACJI

Damix Spółka z ograniczoną odpowiedzialnością

z siedzibą w Rypinie

KRS: 0000124512 NIP: 8921196255

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w przedsiębiorstwie, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Definicje:

1. **Administrator Danych Osobowych (Administrator)** - DAMIX Spółka z ograniczoną odpowiedzialnością z siedzibą w Rypinie.
2. **Dane osobowe** - wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby 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 identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
3. **Dane osobowe wrażliwe** - szczególne kategorie danych określone w art. 9 RODO, w tym: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby; jak również dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa, o których mowa w art. 10 RODO.

4. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
5. **Obszar przetwarzania danych osobowych** – pomieszczenia lub części pomieszczeń we wszystkich lokalizacjach przedsiębiorstwa, w których są przetwarzane dane osobowe, zarówno w formie papierowej, jak i w systemie informatycznym.
6. **Odbiorca danych** – podmiot, któremu udostępniane są dane osobowe.
7. **Osoba upoważniona** – osoba upoważniona do przetwarzania danych osobowych przez Administratora danych lub osobę przez niego upoważnioną, mająca bezpośredni dostęp do danych, przetwarzanych w systemie informatycznym lub w dokumentacji papierowej.
8. **Podmiot przetwarzający** – podmiot, któremu przedsiębiorstwa powierza czynności przetwarzanie danych osobowych w swoim imieniu.
9. **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
10. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.
11. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych.

12. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
13. **UODO** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018, poz. 1000).
14. **Zasób danych osobowych** - wszystkie dane osobowe, niezależnie od sposobu ich utrwalenia, zarówno w formie elektronicznej - w systemie informatycznym oraz na nośnikach (płyty CD/DVD/BD, pamięci flash i inne) jak i papierowej przetwarzane DAMIX Spółkę z ograniczoną odpowiedzialnością w celu realizacji jej zadań.

§ 1
Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w przedsiębiorstwie DAMIX Spółka z ograniczoną odpowiedzialnością, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

§ 2

Zasady zbierania danych osobowych

1. Dane osobowe przetwarzane przez Administratora gromadzone są w zbiorach danych.
2. DAMIX Spółka z ograniczoną odpowiedzialnością uzyskuje dane osobowe przede wszystkim bezpośrednio od swoich Klientów oraz Pracowników.
3. DAMIX Spółka z ograniczoną odpowiedzialnością uzyskuje dane osobowe, w szczególności, w zakresie:

   a) informacji kontaktowych (imię, nazwisko, adres korespondencyjny/prowadzenia działalności gospodarczej, e-mail oraz numer telefonu),

   b) służbowych informacji kontaktowych (stanowisko, dział, nazwa instytucji),

   c) potrzebnych do wystawienia faktury VAT (NIP, REGON).

   d) dane o NFZ, stopniu niepełnosprawności, wykształceniu, zawodzie, nr rachunku bakowego, prawie do emerytury

§ 3

Sposób przetwarzania danych osobowych u Administratora

1. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:

   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,

   b) kontrolę i nadzór nad przetwarzaniem danych osobowych,

   c) monitorowanie zastosowanych środków ochrony.
2. Monitorowanie przez Administratora zastosowanych środków ochrony obejmuje m.in. działania osób upoważnionych, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

3. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.
4. Administrator nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
5. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
6. Administrator prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

§ 4
Upoważnienie osób do przetwarzania danych osobowych

1. Wszystkie osoby, które wykonują czynności związane z przetwarzaniem danych osobowych w DAMIX Spółce z ograniczoną odpowiedzialnością, w ramach wykonywania zadań służbowych na stanowiskach pracy lub prac zleconych, muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych oraz podpisać oświadczenie o zachowaniu tajemnicy danych oraz sposobów ich zabezpieczenia.
2. Wzór upoważnienia oraz oświadczenia stanowi załącznik nr 2 do niniejszej polityki.
3. Upoważnienia do przetwarzania danych osobowych nadaje Administrator.
4. Upoważnienia do przetwarzania danych są przygotowywane i przechowywane przez Administratora.

§ 5

Podstawowe zasady, które powinny przestrzegać osoby upoważnione do przetwarzania danych osobowych

1. Osoba upoważniona do przetwarzania danych osobowych w DAMIX Spółce z ograniczoną odpowiedzialnością jest zobowiązana do:
   a) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz dokumentacją dotyczącą ochrony danych osobowych w DAMIX Spółka z ograniczoną odpowiedzialnością;
   b) przetwarzania danych osobowych wyłącznie w celu i zakresie wynikającym z nałożonych obowiązków służbowych lub zleconych zadań;
   c) zachowania wyjątkowej staranności przy przetwarzaniu danych osobowych, w szczególności danych wrażliwych w celu ochrony interesów osób, których dane dotyczą;
   d) stosowania określonych w DAMIX Spółce z ograniczoną odpowiedzialnością procedur i środków przetwarzania oraz zabezpieczania danych osobowych;
   e) podporządkowania się poleceniom Administratora w zakresie ochrony danych osobowych;
   f) zachowania w poufności danych osobowych oraz danych objętych tajemnicą przedsiębiorstwa;
   g) zabezpieczenia danych osobowych przed: ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub ich udostępnieniem osobom nieupoważnionym;
   h) dopilnowania, aby przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej;
   i) dopilnowania, aby przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie - zabronione jest wyrzucanie dokumentów do koszy na śmieci bez ich właściwej anonimizacji;

j) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;

k) zachowania należytej staranności podczas przekazywania danych osobowych drogą telefoniczną (konieczność właściwej identyfikacji rozmówcy, konieczność ustalenia, czy rozmówca jest uprawniony do pozyskania danych osobowych, przekazywanie jedynie niezbędnych informacji);

l) przesyłania danych osobowych za pomocą sieci Internet jedyne z użyciem metod kryptograficznych (szyfrowanie danych, kanały bezpiecznej transmisji);

m) niewysyłania za pomocą wiadomości e-mail danych osobowych na prywatne adresy, niekopiowanie danych na inne nośniki bez uzasadnionej potrzeby biznesowej;

n) zachowania należytej ostrożności przy transporcie dokumentów oraz nośników informatycznych, zawierających dane osobowe, poza obszarem przetwarzania w DAMIX Spółce z ograniczoną odpowiedzialnością;

o) niepozostawiania dokumentów, zawierających dane osobowe na urządzeniach wielofunkcyjnych (drukowanie, kopiowanie);

p) nieopuszczania stanowiska bez zabezpieczenia dokumentów papierowych, zawierających dane osobowe (zasada „czystego biurka") oraz bez zabezpieczania dostępu do danych przetwarzanych w systemie informatycznym (zasada „czystego ekranu");

q) informowania o zdarzeniu operacyjnym dotyczącym danych osobowych, zgodnie z obowiązującymi w tym zakresie procedurami;

r) zaprzestania przetwarzania danych osobowych po ustaniu stosunku zatrudnienia.

§ 6

Realizacja obowiązków przy przetwarzaniu danych osobowych

1. Osoby odpowiedzialne w DAMIX Spółce z ograniczoną odpowiedzialnością za procesy, w których zbierane są dane osobowe, mają obowiązek zachowania szczególnej staranności przy ich zbieraniu, w tym:
   a) sprawdzać czy są spełnione podstawy prawne na pozyskiwanie danych osobowych, zgodnie z art. 6 RODO oraz art. 9 - 10 RODO;
   b) zbierać dane osobowe dla określonych, zgodnych z prawem celów realizowanych w DAMIX Spółka z ograniczoną odpowiedzialnością;
   c) zbierać dane w zakresie adekwatnym do celów w jakich dane będą przetwarzane w DAMIX Spółce z ograniczoną odpowiedzialnością.
2. W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadamiać o prawie do odwołania takiej zgody.
3. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO.
4. Dane osobowe zbierane w ramach procesów realizowanych w DAMIX Spółce z ograniczoną odpowiedzialnością są przetwarzane przez czas określony przez właściwe przepisy prawa lub wewnętrzne przepisy kancelaryjno-archiwalne.
5. Za określenie odpowiednich czasów retencji danych osobowych w procesach przetwarzania danych odpowiada Administrator.
6. Dane osobowe, dla których okres przetwarzania nie wynika z obowiązujących przepisów prawa i dla których nie jest możliwe określenie z góry tego okresu w wewnętrznych przepisach kancelaryjno - archiwalnych, są przetwarzane tak długo, jak długo istnieje jednocześnie podstawa prawna oraz cel dla ich przetwarzania.

7. Ustanie celu przetwarzania danych jest równoznaczne z koniecznością usunięcia danych osobowych.
8. Dane osobowe przetwarzane wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody.
9. Osoby, które udostępniają w imieniu DAMIX Spółki z ograniczoną odpowiedzialnością dane osobowe do podmiotu zewnętrznego (w formie papierowej lub elektronicznej), przed ich udostępnieniem mają obowiązek sprawdzić czy istnieją podstawy prawne umożliwiające wykonanie tych czynność, w tym:
   a) wymóg prawa dotyczący udostępnienia danych;
   b) zgoda osoby na udostępnienie danych innemu podmiotowi;
   c) zapis w umowie z podmiotem współpracującym, przy spełnieniu warunku, że udostępnienie nie narusza praw i wolności osoby, której dane dotyczą;
   d) wniosek o udostępnienie danych od podmiotu uprawnionego, ze wskazaniem podstawy prawnej do otrzymywania danego rodzaju danych osobowych.
10. Każda sytuacja dotycząca udostępnienia danych osobowych musi być konsultowana z Administratorem.

§ 7
Powierzenie czynności przetwarzania danych osobowych

1. W sytuacji powierzania czynności przetwarzania danych osobowych zewnętrznemu podmiotowi (podmiotowi przetwarzającemu), należy zawrzeć z nim umowę powierzenia przetwarzania danych osobowych zgodnie z art. 28 ust. 3 RODO.
2. W trakcie dokonywania wyboru podmiotu przetwarzającego należy zweryfikować czy podmiot ten zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie

spełniało wymogi przepisów RODO i chroniło prawa osób, których dane dotyczą.

3. Umowę z podmiotem zewnętrznym, któremu zlecone zostanie wykonywanie czynności związanych z przetwarzaniem danych osobowych przygotowuje Administrator.
4. Wzór umowy powierzenia znajduje się w Załączniku nr 3 do niniejszej Polityki.
5. Kontrola podmiotów przetwarzających, którym zostały powierzone czynności przetwarzania danych osobowych należących do DAMIX Spółki z ograniczoną odpowiedzialnością jest przeprowadzana przez Inspektora lub inne wyznaczone osoby zgodnie z zapisami zawartymi w umowach powierzenia przetwarzania danych osobowych, w odniesieniu do uprawnienia określonego w art. 28 ust. 3 lit. h RODO.

§ 8
Przekazywanie danych osobowych do podmiotu znajdującego się w państwie trzecim

W sytuacji przekazywania danych osobowych do podmiotu znajdującego się w państwie trzecim (poza Europejskim Obszarem Gospodarczym) należy taką sytuację skonsultować z Administratorem.

§ 9
Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie DAMIX Spółki z ograniczoną odpowiedzialnością, obejmuje pomieszczenia biurowe i handlowe przedsiębiorstwa zlokalizowane w Rypinie przy ul. Bohaterów Czerwca 1956 r. nr 3, a także w oddziałach Spółki, o ile istnieją.

2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

§ 10

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, Środki obejmują:
    a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.
    b) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w § 8 na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
    c) Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
    d) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
    e) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.
    f) Ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem.
    g) Zabezpieczenie dostępu do urządzeń DAMIX Spółki z ograniczoną odpowiedzialnością przy pomocy haseł dostępu.

h) Wykorzystanie szyfrowania danych przy ich transmisji.

§ 11
Naruszenie zasad ochrony danych osobowych

1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   g) naruszenie praw osób, których dane są przetwarzane.
2. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Osoba Upoważniona zobowiązana jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora,
3. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
4. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki

– jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

5. Wzór zgłoszenia określa załącznik nr 4 do niniejszej polityki.
6. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

§ 12
Postanowienia końcowe

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Administrator jest obowiązany zapoznać z treścią Polityki swoich pracowników i współpracowników.
3. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz UODO.
4. Pracownicy i współpracownicy DAMIX Spółki z ograniczoną odpowiedzialnością zobowiązani są do bezwzględnego stosowania zasad określonych w Polityce.

Załączniki:

1. Wzór rejestru czynności przetwarzania.
2. Wzór upoważnienia wraz z oświadczeniem.
3. Wzór umowy powierzenia.
4. Wzór zgłoszenia incydentu naruszenia ochrony danych osobowych.
5. Wzór rejestru naruszeń.
6. Wzór wykazu budynków.
7. Wykaz zbiorów danych.
8. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Adam Krzemiński
Wiceprezes Zarządu

Załącznik nr 1

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
															Transfer do kraju trzeciego lub org. międzynarodowej	
LP	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	Kategorie odbiorców (jeśli inni niż podmiot przetwarzający)	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer z art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
1																
2																
3																
4																
5																
6																
7																

Załącznik nr 2

Rypin, dnia ____ r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH[1]

Nr __/__/___

Niniejszym upoważniam _____

Stanowisko: _____

do przetwarzania danych osobowych w DAMIX Spółce z ograniczoną odpowiedzialnością z siedzibą w Rypinie:

A. Okres upoważnienia:

- w okresie trwania _____ do dnia _____ r.;

B. Zakres upoważnienia:

- dane przetwarzane na nośnikach papierowych:

  _____

- system informatyczny oraz urządzenia wchodzące w jego skład:

  _____

- (bez ograniczeń*, podgląd danych*, wprowadzanie danych*, opracowywanie danych*, zmienianie danych*, usuwanie danych*, na komputerach przenośnych*).
- dane osobowe objęte zbiorem:

  _____

_____

podpis Pracodawcy

_____

*niepotrzebne przekreślić

OŚWIADCZENIE OSOBY UPOWAŻNIANEJ

Oświadczam, iż zostałam / zostałem* zaznajomiony z treścią upoważnienia oraz przepisami o ochronie danych osobowych i dokumentacją w sprawie przetwarzania i ochrony danych osobowych. Zobowiązuję się do przetwarzania danych wyłącznie w zakresie nadanego upoważnienia, a także do zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia.

_____

data i podpis Pracownika

*niepotrzebne przekreślić

Załącznik nr 3

Umowa
o powierzenie przetwarzania danych osobowych

zawarta w dniu _____ w _____ pomiędzy:

DAMIX Spółką z ograniczoną odpowiedzialnością z siedzibą w Rypinie przy ul. Bohaterów Czerwca 1956 r. nr 3 wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy w Toruniu po numerem KRS: 000012451, NIP: 8921196255, REGON: 910301250, kapitał zakładowy 1 460 000,00 zł,
reprezentowaną przez
_____ - _____
_____-_____
zwaną w dalszej części umowy **Administratorem**

a

_____
__,
zwaną w dalszej części umowy **Przetwarzającym**
-

Strony zgodnie oświadczają, że

a) łączy je umowa, w związku z której wykonywaniem Administrator powierzył Przetwarzającemu przetwarzanie danych osobowych;
b) w związku z zawarciem ww. umowy, istnieje konieczność uregulowania zasad przetwarzania danych osobowych w sposób zgodny z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1), zwanym w dalszej części umowy RODO.

W tym stanie rzeczy, Strony zawierają umowę celem uregulowania warunków, na jakich Przetwarzający wykonywać będzie operacje przetwarzania danych osobowych w imieniu i na rzecz Administratora, o następującej treści:

§ 1.
Przedmiot Umowy

1. Niniejsza umowa określa zasady oraz podstawy powierzenia Przetwarzającemu przetwarzania danych osobowych, a to w celu wykonania zobowiązań wobec Administratora, o których mowa w art. 28 RODO.

2. Na warunkach określonych niniejszą umową, Administrator powierza Przetwarzającemu przetwarzanie danych osobowych, a Przetwarzający się zobowiązuje się do przetwarzania powierzonych danych osobowych zgodnego z RODO oraz przepisami prawa obowiązującymi na terenie Unii Europejskiej, przy czym Przetwarzający oświadcza, że dysponuje środkami technicznymi, doświadczeniem i wiedzą, co umożliwi jemu prawidłowe wykonanie niniejszej umowy.

§ 2.
Przetwarzanie danych osobowych oraz wykonywanie innych obowiązków wynikających z RODO

1. Strony zgodnie postanawiają, iż przetwarzanie powierzonych przez Administratora na rzecz Przetwarzającego danych osobowych odbywać się będzie zgodnie z RODO i w szczególności nie może naruszać następujących zasad:
   a) Przetwarzający uprawniony jest do przetwarzania danych osobowych wyłącznie w zakresie i celu ustalonym przez Strony niniejszej umowy i będzie wykonywane w okresie jej obowiązywania, przy czym Przetwarzający będzie uprawniony do przetwarzania danych osobowych również po jej rozwiązaniu, ale tylko w zakresie, w którym przetwarzanie danych osobowych jest niezbędne dla ochrony interesów prawnych Administratora, Przetwarzającego, w tym w szczególności dla wykonania obowiązków publicznoprawnych Administratora oraz Przetwarzającego wynikających z prawa podatkowego lub ubezpieczeń społecznych, tj.: w odniesieniu do danych zwykłych: imię i nazwisko, numer ewidencyjny PESEL, adres zamieszkania, adres e-mail, numery telefonów, data urodzenia, NIP, REGON, numer wpisu do KRS, seria i numer dokumentu tożsamości, numer rachunku bankowego, a także w odniesieniu do danych osobowych niestrukturyzowanych: informacje o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe oraz elektroniczne, obrazy, nagrania, filmy);
   b) Przetwarzający przetwarzać będzie dane następujących kategorii osób: klientów Administratora, a także innych osób, co do których niezbędne jest uzyskanie ich danych osobowych w związku z wykonywaniem umowy łączącej Przetwarzającego z Administratorem;
   c) przetwarzanie będzie odbywało się przy wykorzystywaniu systemów informatycznych oraz w formie dokumentów papierowych;
   d) powierzenie przetwarzania przez Administratora na rzecz Przetwarzającego następuje w celu realizacji umowy łączącej Strony, przy czym obejmować będzie ono jedynie dane zwykłe;
   e) Przetwarzający uprawniony będzie do przekazania danych osobowych innym podmiotom w celu realizacji niniejszej umowy, _____ .
2. Przetwarzający zobowiązany jest, we współpracy z Administratorem, do stosowania środków zabezpieczających powierzone jemu dane osobowe zgodnie z RODO, w szczególności uwzględniając przy tym wiedzę techniczno - informatyczną oraz cele przetwarzania, a także ryzyka naruszania praw lub wolności osób fizycznych. Przetwarzający obowiązany jest zastosować środki techniczne i organizacyjne

zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić optymalny stopień bezpieczeństwa, co powinno udokumentowane poprzez złożenie stosownego oświadczenia przez Przetwarzającego zawierającego opis środków techniczno - informatycznych. Na żądanie Administratora, Przetwarzający umożliwi dokonanie jemu stosownego audytu w zakresie i terminach wskazanych przez Administratora.

3. Przetwarzający zobowiązany jest zapewnić, aby osoby zatrudnione przy przetwarzaniu danych osobowych, przetwarzały je wyłącznie w celach określonych w niniejszej umowie, a także aby w okresie jej obowiązywania posiadały stosowne upoważnienia do przetwarzania danych osobowych i zachowały je oraz sposoby zabezpieczeń w tajemnicy.
4. W przypadku wykrycia przez Przetwarzającego naruszenia przez osoby trzecie ochrony danych osobowych, zobowiązany jest on w terminie jednej doby od wykrycia takiego zdarzenia do podjęcia czynności umożliwiających wywiązanie się przez Administratora z obowiązków informacyjnych wynikających z art. 32 i następnych RODO, a w szczególności przygotowania informacji wymaganych w zgłoszeniu naruszenia ochrony danych do organu nadzorczego (PUODO) oraz prowadzenia rejestru naruszeń ochrony danych osobowych.
5. Przetwarzający zobowiązany jest również do zapewnienia wsparcia Administratora poprzez odpowiednie środki techniczne i organizacyjne, w wykonywaniu obowiązków reakcji na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w Rozdziale III RODO, a dotyczących w szczególności raportowania zakresu przetwarzanych danych osobowych, sprostowania danych osobowych, ograniczenia przetwarzania, zgłoszenia sprzeciwu w zakresie przetwarzania danych osobowych.
6. Strony niniejszej umowy zobowiązane są do współpracy z organem nadzorczym (PUODO) w zakresie wykonywanych przez niego zadań. Przetwarzający zobowiązuje się stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.
7. Przetwarzający nie jest uprawniony do przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej poza Europejski Obszar Gospodarczy. Jeżeli przy wykonywaniu niniejszej umowy Przetwarzający poweźmie zamiar lub będzie mieć obowiązek przekazywać dane osobowe poza Europejski Obszar Gospodarczy, Przetwarzający zobowiązany jest pisemną zgodę Administratora.

§ 3.
Odpowiedzialność Przetwarzającego za naruszenia ochrony danych osobowych

1. Przetwarzający jest odpowiedzialny wobec Administratora oraz osób, których dane osobowe są przetwarzane za szkody spowodowane swoim działaniem lub zaniechaniem w związku z naruszenie przepisów RODO, a także w przypadku działania naruszającego zalecania Administratora, w tym w przypadku zastosowania lub niezastosowania właściwych środków bezpieczeństwa.

2. Przetwarzający zobowiązany jest również do niezwłocznego poinformowania Administratora o wszelkich wątpliwościach, co do zgodności z prawem wydanych przez zaleceń lub instrukcji, które w jego ocenie stanowią naruszenie RODO lub przepisów prawa obowiązujących na terenie Unii Europejskiej, a to pod rygorem odpowiedzialności odszkodowawczej.

§ 4.
Podpowierzenie

1. Przetwarzający może powierzyć konkretne operacje przetwarzania danych osobowych (**podpowierzenie**) w drodze pisemnej umowy innym podmiotom przetwarzającym pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.
2. Powierzenie przetwarzania danych osobowych Podprzetwarzającym wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia danych osobowych konkretnemu Podprzetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć danych osobowych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.
3. Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej umowy, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.
4. Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.
5. Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania umowy.

§ 5.
Rozwiązanie umowy

1. Niniejsza umowa została zawarta na czas obowiązywania umowy _____. W przypadku rozwiązania tej umowy, niniejsza umowa ulega rozwiązaniu bez potrzeby składania dodatkowych oświadczeń przez jej Strony.
2. Przetwarzający zobowiązuje się w terminie jednego miesiąca po zakończeniu świadczenia usług na rzecz Administratora, w zależności od jego decyzji do usunięcia

lub zwrócenia Administratorowi wszelkich danych osobowych, chyba że ich dalsze przetwarzanie jest uzasadnione prawem obowiązującym w Unii Europejskiej. Po usunięciu ww. danych osobowych, Przetwarzający złoży stosowne pisemne oświadczenie o wykonaniu obowiązku usunięcia lub zwrócenia powierzonych danych osobowych.

§ 6.
Postanowienia końcowe

1. Wszelkie zmiany lub uzupełnienia do Umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych postanowieniami Umowy odpowiednie zastosowanie znajdują postanowienia RODO oraz powszechnie obowiązującego prawa polskiego.
3. Strony zgodnie poddają wszelkie spory mogące wyniknąć z niniejszej umowy właściwemu Sądowi w Toruniu.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej Stron.

Podpisy stron zawierających umowę oraz daty złożenia podpisów

ADMINISTRATOR **PRZETWARZAJĄCY**

Załącznik nr 4

Rypin, dnia _____ r.

Prezes Urzędu Ochrony Danych Osobowych

_____

_____

ZGŁOSZENIE INCYDENTU NARUSZENIA DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

1. Administrator Danych Osobowych _____
2. Miejsce i dzień naruszenia _____
3. Kategoria i przybliżona liczba osób, których dane dotyczą _____
4. Kategoria i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie _____
5. Opis charakteru naruszenia ochrony danych _____
6. Możliwe konsekwencje naruszenia ochrony danych _____
7. Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych _____

Załącznik nr 5 – wzór rejestru naruszeń

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

Załącznik nr 6

Wykaz budynków, pomieszczeń lub części pomieszczeń

tworzących obszar, w którym są przetwarzane dane osobowe

L.p.	Lokalizacja - adres i numer budynku	Numer pomieszczenia/przeznaczenie	Uwagi
1.			
2.			
3.			
4.			

Załącznik nr 7 do Polityki Bezpieczeństwa:

Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania

Lp.	Nazwa zbioru danych osobowych	System zastosowany do przetwarzania /nazwa systemu informatycznego/	Zakres danych osobowych w zbiorze danych /kategorie danych/	Komunikacja z innymi systemami (T/N)	Przepływ danych
1.	Zbiór danych klientów i kontrahentów	dane w postaci dokumentów WORD, PDF, dane w postaci papierowej wykaz w postaci arkusza kalkulacyjnego	• Imiona i nazwiska • Miejsce urodzenia • Adres zamieszkania/pobytu/prowadzenia działalności gospodarczej • Numer telefonu • Adres e-mail • NIP • REGON • numer rachunku bankowego		
2.	Zbiór danych pracowników i współpracowników	dane w postaci dokumentów WORD, PDF, dane w postaci papierowej wykaz w postaci arkusza kalkulacyjnego	• Imiona i nazwiska • Imiona rodziców • Data i miejsce urodzenia • Miejsce zamieszkania lub pobytu • Wykształcenie, zawód, miejsce pracy • PESEL • Numer telefonu • Adres e-mail • Numer rachunku bankowego		
3.	Zbiór danych kandydatów do pracy	dane w postaci dokumentów WORD, PDF, dane w postaci papierowej wykaz w postaci arkusza kalkulacyjnego	• imię (imiona) i nazwisko • imiona rodziców • datę urodzenia • miejsce zamieszkania (adres do korespondencji) • wykształcenie • przebieg dotychczasowego zatrudnienia		
4.	Zbiór danych wspólników i osób reprezentujących Spółkę	dane w postaci dokumentów WORD, PDF, dane w postaci papierowej wykaz w postaci arkusza kalkulacyjnego	• Imiona i nazwiska • Imiona rodziców • Data i miejsce urodzenia • Miejsce zamieszkania lub pobytu • Wykształcenie, zawód, miejsce pracy • PESEL • Numer telefonu • Adres e-mail • Numer rachunku bankowego		
5.	Rejestr korespondencji	dane w postaci dokumentów WORD, PDF, dane w postaci papierowej wykaz w postaci arkusza kalkulacyjnego	• Imiona i nazwiska • Miejsce zamieszkania/pobytu/prowadzenia działalności gospodarczej		
6.			•		

Załącznik nr 8

Wykaz osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zbiory danych, które obejmuje upoważnienie
1.				