MAXPOL Tworzymy ludzi i kapitał
DORADZTWO I POŚREDNICTWO HANDLOWE

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

MAXPOL PAWEŁ POLKOWSKI

ORLA 11 SZCZĘSNE 05-825 GRODZISK MAZOWIECKI

I. W Polityce Bezpieczeństwa użyto następujących definicji

1.	**Administrator**	**Maxpol Paweł Polkowski ul. Orla 11 Szczęsne 05-825 Grodzisk Mazowiecki**
2.	**Dane osobowe**	oznaczają wszelkie 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
3.	**Poufność danych**	ochrona danych osobowych przed dostępem tych danych przez osoby nieupoważnione
4.	**Przetwarzanie danych osobowych**	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
5.	**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
	Ustawa	Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku
6.	**System informatyczny/system IT**	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
7.	**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
8.	**Wniosek podmiotu danych**	Wniosek osoby fizycznej dotyczący realizacji swoich praw na gruncie RODO

9.	**Podmiot danych**	Inaczej właściciel danych, czyli osoba, której dane dotyczą
10.	**Rozliczalność**	Właściwość, która umożliwia wykazanie zgodności Administratora z przepisami o ochronie danych osobowych w tym RODO oraz Ustawy
11.	**Polityka**	Niniejszy dokument- Polityka bezpieczeństwa danych osobowych

II. Zasady ogólne dotyczące bezpieczeństwa przetwarzanych danych osobowych

1. Celem Polityki Bezpieczeństwa jest opracowanie oraz wskazanie zasad jakie powinny być przestrzegane w celu zapewnienia ochrony, poufności i integralności danych osobowych.
2. Polityka Bezpieczeństwa ma na celu zagregować i opisać stosowane w strukturach Administratora zabezpieczenia techniczne i organizacyjne w celu ochrony danych osobowych.
3. Polityka Bezpieczeństwa ma na celu udokumentować rozliczalność Administratora co do stosowania przepisów o ochronie danych osobowych i stanowi podstawę do wdrożenia pozostałych procedur i zabezpieczeń.
4. Podstawą prawną stosowania niniejszej Polityki jest 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 jak również Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku.

III. Obowiązek przetwarzania danych w zgodzie z przepisami prawa

1. Administrator przetwarza dane osobowe tylko i wyłącznie na podstawie przesłanek przetwarzania danych osobowych określonych w art. 6 RODO.

2. Administrator jest zobowiązany do wskazania podstawy prawnej (z RODO) legalizującej przetwarzania takich danych.
3. Administrator, zbierając dane osobowe, w momencie ich zbierania bezpośrednio od właściciela danych, jest on zobowiązany poinformować właściciela danych (np. poprzez przedstawienie odpowiedniego klauzuli) zgodnie z ***Polityką prywatności.***
4. W przypadku zbierania danych od osób trzecich, właściciela danych należy poinformować niezwłocznie po utrwaleniu danych o okolicznościach przetwarzania zgodnie z art. 14 RODO.
5. W przypadku korzystania z systemów informatycznych, które automatycznie zbierają dane osobowe należy zapewnić, aby system ten udzielał informacji, o której mowa w pkt. powyżej.

IV. Powierzenie przetwarzania danych osobowych

1. Jeśli Administrator podejmie decyzję o korzystaniu z usług podmiotu trzeciego w ramach świadczenia tych usług podmiot ten będzie przetwarzał dane osobowe na zlecenie lub w imieniu Administratora, to należy zapewnić, aby przed przekazaniem danych temu podmiotowi, została zawarta „*Umowa powierzenia przetwarzania danych osobowych*" oraz podmiot ten został odpowiednio zweryfikowany zgodnie z ***Procedurą wyboru podmiotu przetwarzającego.***

V. Realizacja wniosków o dostęp do danych

1. Jeśli właściciel danych zgłosi się z ustnym lub pisemnym wnioskiem / prośbą o dostęp / kopię danych / przeniesienie danych / usunięcie jego danych / sprostowanie / ograniczenie / zaktualizowanie (niezależnie od formy zgłoszenia papierowo lub elektronicznie), wniesienie sprzeciwu czy wycofania zgody należy niezwłocznie, maksymalnie w ciągu 30 dni

zrealizować taki wniosek zgodnie z ***Procedurą obsługi wniosków podmiotów danych.***

2. Jeśli Administrator nie możne wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. Administrator odmawia podjęcia działań na żądanie osoby, której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15–22 RODO.

VI. Skargi na przetwarzanie danych osobowych/wnioski

1. W przypadku pisemnej skargi / wniosku (niezależnie od formy doręczenia czy zatytułowania) przesłanej przez właściciela danych do Administratora, należy rozpatrzyć niezwłocznie, nie dłużej niż w terminie nie przekraczającym 30 dni od daty wpłynięcia.
2. Odpowiedź na skargę / wniosek należy udzielić na piśmie (przesyłką rejestrowaną) jeśli wnoszący podał adres do doręczeń natomiast w przypadku braku takiego adresu tą samą drogą, którą skarga / wniosek został złożona, chyba, że wnioskujący poprosił o inną formę.

VII. Zasady przetwarzania danych osobowych przez Administratora

1. **Zasada legalności, rzetelności i przejrzystości**

   Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Nie wolno przetwarzać danych osobowych bez podstawy prawnej. Przed przystąpieniem do przetwarzania nowej kategorii danych osobowych lub danych w nowym celu należy wskazać podstawę prawną do ich przetwarzania.

2. **Zasada minimalizacji danych**

Dane osobowe muszą być przetwarzane wyłącznie w konkretnym i jasno sprecyzowanym celu, a właściciel danych musi być o tym celu poinformowany. Dane osobowe musza być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

3. **Zasada minimalizacji**

Można zbierać tylko tyle danych, ile jest adekwatne do realizacji celu. Nie można zbierać „na zapas" ze względu na to, że w przyszłości się „przydadzą". Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

4. **Zasada prawidłowości**

Wszystkie osoby upoważnione do przetwarzania i Podmioty przetwarzające odpowiadają za poprawność merytoryczną danych. Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

5. **Zasada ograniczenia przetwarzania**

Można przetwarzać dane osobowe tylko tak długo jak długo istnieje cel przetwarzania lub określają to przepisy prawa. Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

6. **Zasada poufności i integralność**

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

7. **Zasada ograniczonego dostępu**

   Dostęp do danych osobowych zawsze musi być ograniczony tylko dla osób upoważnionych. Ograniczanie dostępu może być organizacyjne (np. wprowadzanie procedur), fizyczne (np. zamykanie na klucz) lub informatyczne (np. stosowanie loginów haseł).

8. **Zasada podwójnego dostępu**

   Dostęp do danych osobowych zawsze musi być ograniczony poprzez zastosowanie minimum **dwóch ograniczeń dostępu** dowolnego rodzaju. (np. drzwi zamykane na klucz i szafy zamykane na klucz).

9. **Zasada czystego biurka**

   Po skończonej pracy, na biurku nie mogą się znajdować żadne dokumenty lub ogólnodostępne nośniki informatyczne zawierające dane osobowe. Wszystkie takie dokumenty / nośniki powinny być zamknięte na klucz w szafach.

10. **Zasada tajemnicy i jakości haseł dostępowych**

    Pod żadnym pozorem nie wolno ujawnić swojego hasła dostępowego. Hasło należy zmienić nie rzadziej niż raz na 90 dni chyba, że system wymusza wcześniejszą zmianę haseł. **Hasło musi mieć minimum 8 znaków w tym duża litera, mała litera, cyfra i znak specjalny.**

VIII. Stosowane środki techniczne i organizacyjne przez Administratora

1. W celu wzmocnienia nadzoru nad procesami przetwarzania danych osobowych zostały wprowadzone środki organizacyjne zabezpieczenia danych (wykaz w odrębnym zestawieniu zabezpieczeń).
2. Dan osobowe przetwarzane w systemach informatycznych są zabezpieczone za pomocą systemów kopii zapasowych nadzorowanych przez Administratora oraz jeśli dotyczy- dostawcę systemów IT.

3. Każdy system IT użytkowany przez Administratora zapewnia, że operacje na danych osobowych można powiązać z użytkownikiem. Dotyczy to zarówno części aplikacyjnej systemu oraz części bazodanowej. W przypadku zakupu nowych systemów IT, dostawca IT musi zapewnić aby w specyfikacji zakupu systemu IT był zapis o spełnieniu przez dostawcę wymagań dotyczących integralności, poufności rozliczalności wprowadzania i korzystania z danych w systemie.
4. W zależności od kategorii, rodzaju, charakteru, celu przetwarzania danych osobowych są stosowane adekwatne środki zabezpieczenia technicznego w tym środków ochrony fizycznej oraz środków ochrony infrastruktury IT (opis zabezpieczeń w oddzielnym zestawieniu).

IX. Wykaz budynków, w których przetwarzane są dane osobowe

LP.	OBSZAR	ADRES / POMIESZCZENNIE	WŁAŚCICEL lub UMOWA NAJMU
1.	Pomieszczenia administracyjne	ul. Orla 11 Szczęsne 05-025 Grodzisk M.	Paweł Polkowski

X. Wykaz oprogramowania IT służącego do przetwarzania danych osobowych

LP.	NAZWA SYSTEMU	GŁÓWNY ADMINISTRATOR SYSTEMU	STRUKTURA SYSTEMU (zakres danych)	UWAGI
1.	Windows/ Office (Excel)	Paweł Polkowski		-