POLITYKA OCHRONY DANYCH OSOBOWYCH

1. **Definicje**
    1. **Administrator -** dr Katarzyna Piszczek prowadząca działalność gospodarczą pod nazwą Pracownia Psychologiczno-Seksuologiczna ID Katarzyna Piszczek z siedzibą w Gdańsku przy ul. Słowackiego 57D/8, 80-257 Gdańsk, NIP: 584-255-04-94.
    2. **Dane osobowe –** informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania przez jeden bądź klika szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość, w tym wizerunek, nagranie głosu, dane kontaktowe, daneo lokalizacji, informacje zawarte w korespondencji, informacje gromadzone za pośrednictwem sprzętu rejestrującego lub innej podobnej technologii.
    3. **Organ nadzorczy –** Prezes Urzędu Ochrony Danych Osobowych lub ewentualnie właściwy organ nadzoru w zakresie Danych osobowych wyznaczony przez inne państwo członkowskie Unii Europejskiej.
    4. **Podmiot danych –** osoba fizyczna, której dotyczą Dane osobowe przetwarzane przez Administratora.
    5. **Polityka –** niniejsza Polityka Ochrony Danych Osobowych.
    6. **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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.U.UE.L.2016.119.1 z późn. zm.

2. **Zasady ogólne**
    1. Niniejsza Polityka stanowi podstawowy dokument regulujący zasady przetwarzania Danych osobowych przez Administratora.
    2. Wdrożenie Polityki ma na celu zapewnienie zgodności z RODO procesów przetwarzania Danych osobowych przez Administratora, bez względu na formę (elektroniczną bądź papierową), w jakiej przetwarzanie następuje.
    3. W związku z prowadzoną działalnością Administrator zbiera i przetwarza Dane osobowe, zgodnie z właściwymi przepisami prawa, w tym w szczególności RODO i przewidzianymi w nich zasadami przetwarzania tj.:
        1. Administrator zapewnia, że przetwarzanie przez niego Danych osobowych jest zgodne z prawem i odbywa się w oparciu o jedną z podstaw przetwarzania określonych w RODO tj. w art. 6 ust. 1, art. 9 ust. 2 albo art. 10 (zasada zgodności z prawem);
        2. Administrator zapewnia rzetelność i przejrzystość przetwarzania Danych osobowych, w szczególności zawsze informuje o przetwarzaniu Danych osobowych w momencie ich zbierania, w tym o celu i podstawie prawnej przetwarzania (zasada rzetelności i przejrzystości);
        3. Administrator zapewnia, że Dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są przetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczenia celu);
        4. Administrator zapewnia, że przetwarza dane wyłącznie w zakresie niezbędnym do realizacji celu, dla którego Dane osobowe zostały zebrane (zasada minimalizacji);
        5. Administrator zapewnia, że przetwarzane przez niego Dane osobowe są prawidłowe i w razie potrzeby będą uaktualniane oraz że podejmuje on wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);
        6. Administrator zapewnia, że Dane osobowe są przetwarzane tylko przez okres, w jakim jest to niezbędne dla zrealizowania celów przetwarzania (zasada ograniczenia czasowego);
        7. Administrator zapewnia bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez wdrożenie odpowiednich środków technicznych lub

organizacyjnych (zasada integralności
i poufności).

4. Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania Danych osobowych z RODO oraz pozostałymi przepisami dotyczącymi Danych osobowych (rozliczalność).

3. **Organizacja systemu ochrony Danych osobowych**
    1. Przed udzieleniem dostępu do przetwarzania Danych osobowych Administrator zapoznaje osoby przetwarzające Dane osobowe z jego upoważnienia z Polityką, w tym procedurami i zasadami dotyczącymi ochrony Danych osobowych obowiązującymi w organizacji Administratora.
    2. Administrator jest odpowiedzialny w szczególności za:
        1. Monitorowanie przestrzegania przez osoby upoważnione przepisów RODO oraz innych przepisów unijnych i krajowych z zakresu ochrony Danych osobowych, jak również wewnętrznych polityk i procedur wdrożonych u Administratora w tym zakresie;
        2. Podejmowanie działań zwiększających świadomość w zakresie ochrony Danych osobowych, w tym osób uczestniczących w operacjach przetwarzania oraz prowadzenie powiązanych z tym audytów;
        3. Udzielenie na żądanie, zaleceń co do oceny skutków dla ochrony Danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
        4. Współpraca z Organem nadzorczym;
        5. Pełnienie funkcji punktu kontaktowego dla Organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których stanowi art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
    3. Administrator wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

4. **Bezpieczeństwo Danych osobowych**

    1. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożeń. Administrator uwzględnia przy tym stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.
    2. Przy ocenie, czy stopień bezpieczeństwa jest odpowiedni, Administrator uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego
    z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
    3. W celu zapewnienia integralności i poufności Danych osobowych Administrator zapewnia dostęp do Danych osobowych jedynie osobom upoważnionym i wyłącznie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania. Administrator stosuje rozwiązania organizacyjne i techniczne w celu zapewnienia, że wszystkie operacje na Danych osobowych są rejestrowane i realizowane tylko przez osoby uprawnione.
    4. Administrator prowadzi na bieżąco analizę ryzyka związanego z przetwarzaniem Danych osobowych
    i monitoruje adekwatność stosownych zabezpieczeń Danych osobowych do identyfikowanych zagrożeń. W razie konieczności Administrator wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa Danych osobowych.
    5. W przypadku, gdy rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed

rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony Danych osobowych. Jeżeli ocena skutków wskazuje, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z Organem nadzorczym.

6. Jeżeli cele, w których Administrator przetwarza Dane osobowe, nie wymagają zidentyfikowania przez niego Podmiotu danych, Administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania Podmiotu danych wyłącznie po to, żeby zastosować się do wymogów RODO.

5. **Naruszenie ochrony Danych osobowych**
    1. Administrator zapewnia zgłaszanie naruszeń ochrony Danych osobowych Organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym celu Administrator w szczególności zobowiązuje wszystkie osoby przetwarzające Dane osobowego do niezwłocznego informowania o każdym dostrzeżonym naruszeniu ochrony Danych osobowych.
    2. Administrator zapewnia, że bez zbędnej zwłoki zawiadamia Podmioty danych o naruszeniu ochrony Danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności.
    3. W każdym wypadku Administrator bada zaistniałe naruszenie i wdraża stosowne organizacyjne i techniczne środki naprawcze.
    4. Administrator dokumentuje wszelkie naruszenia ochrony Danych osobowych, w tym okoliczności naruszenia ochrony Danych osobowych, jego skutki oraz podjęte działania zaradcze.

6. **Realizowanie uprawnień Podmiotów danych**
    1. Administrator zapewnia, że realizuje uprawnienia Podmiotów danych na zasadach określonych w RODO, w tym prawo do:
        1. **dostępu** – uzyskania od administratora potwierdzenia, czy przetwarzane są jej dane osobowe. Jeżeli dane o osobie są przetwarzane, jest ona uprawniona do uzyskania dostępu do nich oraz uzyskania następujących informacji: o celach przetwarzania, kategoriach danych osobowych, odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, o okresie przechowywania danych lub o kryteriach ich ustalania, o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych przysługujących osobie, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania (art. 15 RODO);
        2. **do otrzymania kopii danych** – uzyskania kopii danych podlegających przetwarzaniu, przy czym pierwsza kopia jest bezpłatna, a za kolejne kopie administrator może nałożyć opłatę w rozsądnej wysokości, wynikającą z kosztów administracyjnych (art. 15 ust. 3 RODO);
        3. **do sprostowania** – żądania sprostowania dot. jej danych osobowych, które są nieprawidłowe lub uzupełnienia niekompletnych danych (art. 16 RODO);
        4. **do usunięcia danych** – żądania usunięcia jej danych osobowych, jeżeli administrator nie ma już podstawy prawnej do ich przetwarzania lub dane nie są już niezbędne do celów przetwarzania (art. 17 RODO);
        5. **do ograniczenia przetwarzania** – żądania ograniczenia przetwarzania danych osobowych (art. 18 RODO), gdy:

i. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
ii. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się ich usunięciu, żądając ograniczenia ich wykorzystywania,
iii. administrator nie potrzebuje już tych danych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
iv. osoba, której dane dotyczą, wniosła sprzeciw wobec przetworzenia – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której

dane dotyczą;

6. **do przenoszenia danych** – otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych jej dotyczących, które dostarczyła administratorowi oraz żądania przesłania tych danych innemu administratorowi, jeżeli dane są przetwarzane na podstawie zgody osoby, której dane dotyczą lub umowy z nią zawartej oraz jeżeli dane są przetwarzane w sposób zautomatyzowany (art. 20 RODO);
7. **do sprzeciwu** – wniesienia sprzeciwu wobec przetwarzania jej danych osobowych w prawnie uzasadnionych celach administratora, z przyczyn związanych z jej szczególną sytuacją, w tym wobec profilowania. Wówczas administrator dokonuje oceny istnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osób, których dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli zgodnie z oceną interesy osoby, której dane dotyczą, będą ważniejsze od interesów administratora, administrator będzie zobowiązany zaprzestać przetwarzania danych w tych celach (art. 21 RODO);
8. **do cofnięcia zgody** w każdym momencie i bez podawania przyczyny, lecz przetwarzanie danych osobowych dokonane przed cofnięciem zgody nadal pozostanie zgodne z prawem. Cofnięcie zgody spowoduje zaprzestanie przetwarzania przez administratora danych osobowych w celu, w którym zgoda ta została wyrażona.

7. **Kontakty z Podmiotem danych**
    1. Administrator wdraża odpowiednie środki, aby komunikacja z Podmiotem danych odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie, jasnym i prostym językiem.
    2. Administrator udziela Podmiotom danych informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli Podmiot danych tego zażąda, Administrator udziela informacji ustnie, o ile jest możliwe potwierdzenie tożsamości Podmiotu danych innymi sposobami.
    3. Administrator ułatwia Podmiotom danych wykonywanie praw przysługujących im na gruncie RODO, w tym uprawnień przewidzianych w art. 15-22 RODO.
    4. Administrator bez zbędnej zwłoki udziela Podmiotom danych informacji o działaniach podjętych w związku z żądaniem zgłoszonym na podstawie art. 15-22 RODO.

8. **Udostępnianie i powierzanie Danych osobowych**
    1. Administrator udostępnia Dane osobowe innemu administratorowi tylko wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 6 ust. 1 albo w art. 9 ust. 2 RODO.
    2. Powierzenie przetwarzania Danych osobowych przez Administratora następuje w oparciu o umowę powierzenia przetwarzania danych lub inny instrument prawny, o którym mowa w art. 28 RODO.
    3. Powierzenie przetwarzania Danych osobowych przez Administratora następuje po uprzedniej weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa Podmiotów danych. Administrator podejmuje ponadto wszelkie niezbędne działania, by także jego podwykonawcy
    i inne podmioty współpracujące dawały gwarancję stosowania odpowiednich środków bezpieczeństwa
    w każdym przypadku, gdy przetwarzają Dane osobowe na zlecenie Administratora.

9. **Przekazywanie Danych osobowych do państw trzecich**
    1. Poziom ochrony Danych osobowych poza Europejskim Obszarem Gospodarczym (EOG) różni się od tego zapewnianego przez prawo europejskie. Z tego powodu Administrator przekazuje Dane osobowe do państwa trzeciego tylko wtedy, gdy jest to konieczne i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:
        1. Współpracę z podmiotami przetwarzającymi Dane osobowe w państwach, w odniesieniu do

których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych osobowych;
2. Stosowania standardowych klauzul umownych wydanych przez Komisję Europejską;
3. W razie przekazywania danych do USA – współpracę z podmiotami uczestniczącymi w programie Tarcza prywatności (*Privacy Shield)* zatwierdzonym decyzją Komisji Europejskiej.

10. **Zapewnienie ciągłości zgodności**
    1. Administrator zapewnia stałe utrzymywanie zgodności działania organizacji z wymaganiami ochrony Danych osobowych przewidzianymi w RODO, w tym weryfikuje i optymalizuje wdrożone w organizacji rejestry i procedury.
    2. W tym celu Administrator między innymi monitoruje zmiany w przepisach prawa, wytyczne krajowych oraz międzynarodowych organów ochrony Danych osobowych oraz orzecznictwo sądów i trybunałów,
    a także uwzględnia najlepsze praktyki rynkowe.

11. **Załączniki**
    1. Administrator prowadzi i stosuje następujące rejestry i procedury dotyczące ochrony Danych osobowych, które stanowią integralną część Polityki:
        1. Procedura retencji danych osobowych;
        2. Procedura obsługi żądań podmiotów danych;
        3. Procedura współpracy z organem nadzorczym.

12. **Postanowienia końcowe**
    1. Polityka wchodzi w życie z dniem 25.05.2018 r.