Polityka Ochrony Danych Osobowych
Dating Show Paweł Kuberski
Flat 2, Stella Court, Coxford Road SO16 5SL
Southampton

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Podmiot przetwarzający w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

- Rozporządzeniu 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 /Dz. Urz. UE.L nr 119, str.1/,
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 2018 r., poz. 1000/,

§1 DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)
Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.
Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania
Anonimizacja - zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych
Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.
Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju

przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.
Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.
Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.
Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.
Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.
Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która 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.
Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

§2

1. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.
2. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Organizacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
3. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

- integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
- dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
- zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§3

Administratorem danych osobowych przetwarzanych w firmie Dating Show Paweł Kuberski jest Paweł Kuberski

§ 4

1. W przedsiębiorstwie przetwarzane są dane osobowe pracowników, kandydatów do pracy, klientów oraz kontrahentów zebrane w zbiorach danych osobowych.
2. ***Informacje te są przetwarzane w postaci dokumentacji elektronicznej.***
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. ***Innymi dokumentami regulującymi ochronę danych osobowych w Przedsiębiorstwie są:***
   a) ***ewidencja osób upoważnionych do przetwarzania danych osobowych,***
   b) ***rejestr czynności przetwarzania danych osobowych,***
   c) ***procedura postępowania w przypadku naruszenia ochrony danych osobowych,***

§ 5

Politykę bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w systemach elektronicznych:
   a) CMS JOOMLA
   b) PHPMYADMIN
   c) Dotpay
   d) Sofort
   e) Paypal
   f) Icash

   wszystkich informacji dotyczących danych klientów i kontrahentów
2. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia
3. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
4. rejestru osób trzecich mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
5. innych dokumentów zawierających dane osobowe.

§ 6

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:
   a. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,

b. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
c. wszystkich osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszystkie osoby mające dostęp do danych osobowych podlegających ochronie.

§ 7

Dane osobowe gromadzone są w*:*

1. Rejestr klientów,
2. Rejestr płatności dokonanych przez klientów
3. Zgody na przetwarzanie danych osobowych
4. Kopie zapasowe nagrań filmowych stworzonych przez klientów portalu
5. Kopie zapasowe rozmów prowadzonych w formie czatu przez klientów portalu
6. Kopie zapasowe wiadomości tekstowych przesyłanych przez klientów portalu
7. Kopie zapasowe zdjęć zamieszczonych przez klientów portalu
8. Rejestr umów powierzenia danych,

§ 8

Zbiory danych osobowych wymienione w § 7 podlegają przetwarzaniu przy użyciu systemów informatycznych wymienionych w § 5 pkt 1 Polityki

§ 9

Dane osobowe przetwarzane są w systemach elektronicznych na serwerze umieszczonym w siedzibie przedsiębiorstwa

§ 10

W przedsiębiorstwie występują następujące zbiory danych osobowych

Lp.	Zbiór danych	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
1.	Rejestr klientów portalu	CMS JOOMLA oraz PHPMYADMIN	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław
2.	Rejestr płatności dokonywanych przez klientów portalu	DOTPAY, ICASH, PAYPAL	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław
3.	Zgody na przetwarzanie danych osobowych udzielone w formie elektronicznej	CMS JOOMLA oraz PHPMYADMIN	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław

4.	Kopie zapasowe nagrań stworzonych przez klientów portalu	CMS JOOMLA oraz PHPMYADMIN	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław
5.	Kopie zapasowe rozmów prowadzonych w formie czatu	AKKEBA BACKUP	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław
6.	Kopie zapasowe wiadomości tekstowych przesyłanych przez klientów portalu	AKKEBA BACKUP	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław
7.	Kopie zapasowe zdjęć zamieszczonych przez klientów portalu	AKKEBA BACKUP	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław
8.	Rejestr umów powierzenia danych	Excel	Zbiór elektroniczny	Serwer, OVH Sp. z o.o. ul. Szkocka 5/1, 54-404 Wrocław

§ 11

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w Organizacji przedstawia się w sposób następujący:

1. *<u>Rejestr klientów</u>*
    1. Nazwa użytkownika
    2. *Imię,*
    3. *Nazwisko*
    4. *Pseudonim*
    5. *Nazwa użytkownika*
    6. *Województwo,*
    7. *adres,*
    8. *Miejscowość zamieszkania,*
    9. *Data urodzenia*
    10. *wiek*
    11. *Stan cywilny*
    12. *Ilość posiadanych dzieci*
    13. *Wykształcenie*
    14. *Sylwetka*

15. *Kolor oczu*
16. *Kolor włosów*
17. *Używki - alkohol, papierosy*
18. *wzrost*
19. *e-mail*
20. *Nr telefonu*
21. *Nr gadu - Gadu lub innego komunikatora*
22. *Data zawarcia umowy,*
23. *Zdjęcia*
24. *Filmy*
25. *Czy klient oczekuje wsparcia finansowego*

2. Rejestr płatności dokonywanych przez klientów portalu
    1. *Imię i nazwisko*
    2. *Adres zamieszkania*
    3. *Nr rachunku bankowego*
    4. *Nr karty kredytowej*

3. Rejestr zgód na przetwarzanie danych
    1. *Imię,*
    2. *Nazwisko,*
    3. *Data wyrażenia zgody*

    ,
4. Kopie zapasowe nagrań filmowych stworzonych przez klientów portalu
    1. Wizerunek
    2. *Imię,*
    3. *Nazwisko,*
    4. *Pseudonim*
    5. *Nazwa użytkownika*
    6. *Województwo,*
    7. *adres,*
    8. *Miejscowość zamieszkania,*
    9. *Data urodzenia*
    10. *wiek*
    11. *Stan cywilny*
    12. *Ilość posiadanych dzieci*
    13. *Wykształcenie*
    14. *Sylwetka*
    15. *Kolor oczu*
    16. *Kolor włosów*
    17. *Używki - alkohol, papierosy*
    18. *wzrost*
    19. *e-mail*
    20. *Nr telefonu*
    21. *Nr Gadu - Gadu lub innego komunikatora*

5. Kopie zapasowe rozmów prowadzonych w formie czatu przez klientów portalu
    1. *Imię,*
    2. *Nazwisko*
    3. *Pseudonim*
    4. *Nazwa użytkownika*
    5. *Województwo,*
    6. *adres,*
    7. *Miejscowość zamieszkania,*
    8. *Data urodzenia*

9. *wiek*
10. *Stan cywilny*
11. *Ilość posiadanych dzieci*
12. *Wykształcenie*
13. *Sylwetka*
14. *Kolor oczu*
15. *Kolor włosów*
16. *Używki - alkohol, papierosy*
17. *wzrost*
18. *e-mail*
19. *Nr telefonu*
20. *Nr Gadu - Gadu lub innego komunikatora*

6. Kopie zapasowe wiadomości tekstowych przesyłanych przez klientów portalu

1. *Imię,*
2. *Nazwisko,*
3. *Województwo*
4. *Pseudonim*
5. *Nazwa użytkownika*
6. *adres,*
7. *Miejscowość zamieszkania,*
8. *Data urodzenia*
9. *wiek*
10. *Stan cywilny*
11. *Ilość posiadanych dzieci*
12. *Wykształcenie*
13. *Sylwetka*
14. *Kolor oczu*
15. *Kolor włosów*
16. *Używki - alkohol, papierosy*
17. *wzrost*
18. *e-mail*
19. *Nr telefonu*
20. *Nr Gadu - Gadu lub innego komunikatora*

7. Kopie zapasowe zdjęć zamieszczonych przez klientów portalu

1. Wizerunek
2. *Imię,*
3. *Nazwisko*
4. *Pseudonim*
5. *Nazwa użytkownika*
6. *Województwo,*
7. *adres,*
8. *Miejscowość zamieszkania,*
9. *Data urodzenia*
10. *wiek*
11. *Stan cywilny*
12. *Ilość posiadanych dzieci*
13. *Wykształcenie*
14. *Sylwetka*
15. *Kolor oczu*
16. *Kolor włosów*
17. *Używki - alkohol, papierosy*
18. *wzrost*

19. *e-mail*
20. *Nr telefonu*
21. *Nr Gadu - Gadu lub innego komunikatora*

Rejestr umów powierzenia danych osobowych

1. Nazwa/ imię nazwisko
2. Numer umowy
3. Data zawarcia umowy
4. Numer telefonu
5. Numer fax
6. Adres e-mail

§ 12

1. Zabezpieczenia organizacyjne
   a. opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
   b. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
   c. opracowano i bieżąco prowadzi się rejestr czynności przetwarzania
   d. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
   e. osoby zajmujące się przetwarzaniem danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
   f. osoby zajmujące się przetwarzaniem danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
   g. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   h. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
   i. dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.
2. Zabezpieczenia techniczne
   a. stanowisko komputerowe wyposażono w indywidualną ochronę antywirusową,
   b. komputer zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,
3. Środki ochrony fizycznej:
   a. urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanej na klucz szafie,
   b. dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

§ 13

Do najważniejszych obowiązków administratora danych osobowych należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,

2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,
3. przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,
4. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
5. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
7. nadzór nad bezpieczeństwem danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

§ 14

1. Administrator systemu informatycznego odpowiedzialny jest za:
   a) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   b) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   c) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
   d) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   e) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   f) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
   g) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   h) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   i) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   j) przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
   k) wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
   l) zarządzanie licencjami, procedurami ich dotyczącymi,
   m) prowadzenie profilaktyki antywirusowej.
2. Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych, oraz Polityki bezpieczeństwa Organizacji przez administratora danych

§ 15

1. Corocznie do dnia 30 czerwca administrator ochrony danych przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych .
2. Sprawozdanie przygotowywane jest w formie pisemnej.

§ 16

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami

wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,

4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.