Ocena Skutków dla Ochrony Danych Osobowych (DPIA)

1. Informacje ogólne

Administrator danych: _____

Osoba dokonująca oceny: _____

Data sporządzenia DPIA: _____

Nazwa projektu/procesu: _____

Opis procesu przetwarzania danych osobowych:

Szczegółowo opisz zakres, cele, sposób i technologię przetwarzania danych (np. system rekrutacji oparty na AI, monitoring wizyjny budynku). Wskaż, jakie dane będą przetwarzane (np. identyfikacyjne, biometryczne, dane o zdrowiu), przez jaki okres (np. dane rekrutacyjne – 6 miesięcy od zakończenia procesu), oraz cel (np. zapewnienie bezpieczeństwa, optymalizacja procesu rekrutacji).

2. Podział procesu na obszary działalności

(przykłady)

- Rekrutacja i zarządzanie personelem (np. systemy ATS, ocena kandydatów z wykorzystaniem AI).

- Marketing i reklama (np. targetowanie w social mediach, analiza danych klientów).

- Monitoring i bezpieczeństwo (np. systemy CCTV, kontrola dostępu).

- Obsługa klienta i sprzedaż (np. formularze kontaktowe, bazy danych klientów).

- Zarządzanie infrastrukturą IT (np. systemy informatyczne, zarządzanie dostępami).

3. Konsultacja z Inspektorem Ochrony Danych

Czy administrator wyznaczył Inspektora Ochrony Danych Osobowych? ☐ Tak ☐ Nie

Jeśli tak, dokumentuj konsultacje z IODO na etapie planowania przetwarzania.

4. Obowiązek przeprowadzenia DPIA

Czy przetwarzanie spełnia co najmniej jedno z poniższych kryteriów? Jeśli tak, DPIA jest obowiązkowa:

- Zautomatyzowane podejmowanie decyzji, w tym profilowanie, wywołujące skutki prawne lub istotne dla osoby fizycznej.

- Przetwarzanie danych szczególnych kategorii lub danych o wyrokach skazujących na dużą skalę.

- Systematyczny monitoring miejsc publicznych.

- Wdrożenie nowych, potencjalnie ryzykownych technologii (np. AI, biometrii).

- Przetwarzanie danych małoletnich lub grup szczególnie chronionych.

5. Ocena ryzyka

Zidentyfikowane zagrożenia *(przykłady):*

- Naruszenie prywatności przez monitoring.

- Dyskryminacja kandydatów przy zastosowaniu AI w rekrutacji.

- Kradzież tożsamości przy wycieku danych.

- Nieuprawnione ujawnienie danych w mediach społecznościowych.

Prawdopodobieństwo ryzyka: ☐ Niskie ☐ Średnie ☐ Wysokie

Poziom ryzyka po zastosowaniu środków zabezpieczających: ☐ Niskie ☐ Średnie ☐ Wysokie

6. Środki minimalizujące ryzyko

Opis zastosowanych środków technicznych i organizacyjnych *(przykłady):*

a) Szyfrowanie danych.

b) Kontrola dostępu i podwójne uwierzytelnianie.

c) Szkolenia pracowników z zakresu RODO i bezpieczeństwa.

d) Pseudonimizacja lub anonimizacja danych.

e) Monitoring dostępu do systemów i logów.

f) Zawarcie umów powierzenia przetwarzania z podmiotami zewnętrznymi.

7. Konsultacja z organem nadzorczym (PUODO)

Czy konieczna jest konsultacja z organem nadzorczym ☐ Tak ☐ Nie

Jeśli mimo zastosowania środków minimalizujących ryzyko pozostaje wysokie, konieczne jest skonsultowanie planowanego przetwarzania z PUODO przed jego rozpoczęciem. W takim przypadku należy przedstawić dokumentację oraz ocenę skutków do PUODO przed rozpoczęciem przetwarzania.

8. Uwzględnienie opinii osób, których dane dotyczą

Czy uwzględniono opinię osób, których dane dotyczą? ☐ Tak ☐ Nie

Jeśli to możliwe i nie narusza to tajemnicy handlowej lub bezpieczeństwa przetwarzania, administrator powinien zasięgnąć opinii osób, których dane dotyczą.

9. Terminy przetwarzania i przeglądu DPIA

(przykłady):

- Dane rekrutacyjne: maksymalnie 6 miesięcy od zakończenia procesu.

- Nagrania z monitoringu: maksymalnie 3 miesiące, chyba że stanowią dowód w postępowaniu.

- Dane marketingowe: do momentu cofnięcia zgody lub wniesienia sprzeciwu.

Przegląd DPIA należy przeprowadzać **nie rzadziej niż co 2 lata** lub każdorazowo w przypadku zmiany procesu, technologii lub oceny ryzyka.

10. Wnioski końcowe

Czy przetwarzanie może zostać rozpoczęte? ☐ Tak ☐ Nie ☐ Po konsultacji z PUODO

Dodatkowe uwagi i zalecenia:

.....
.....
.....