Polityka Ochrony Danych [PRZYKŁAD]

1. Wprowadzenie

1.1. **Cel dokumentu:** Niniejsza Polityka Ochrony Danych określa zasady i procedury przetwarzania danych osobowych w [NAZWA FIRMY], zgodnie z Rozporządzeniem o Ochronie Danych Osobowych (RODO).

1.2. **Zakres stosowania:** Polityka ma zastosowanie do wszystkich pracowników, współpracowników i podwykonawców [NAZWA FIRMY]., którzy mają dostęp do danych osobowych.

1.3. Definicje:

i. **Dane osobowe:** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

ii. **Przetwarzanie:** operacja lub zestaw operacji wykonywanych na danych osobowych.

1.4. **Administrator danych:** [NAZWA FIRMY], adres: [ADRES].

2. Zasady przetwarzania danych osobowych

2.1. **Legalność, rzetelność i przejrzystość:** Przetwarzamy dane osobowe zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

2.2. **Ograniczenie celu:** Zbieramy dane osobowe wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach.

2.3. **Minimalizacja danych:** Ograniczamy zakres przetwarzanych danych do niezbędnego minimum.

2.4. **Prawidłowość:** Dbamy o aktualność i poprawność przetwarzanych danych osobowych.

2.5. **Ograniczenie przechowywania:** Przechowujemy dane osobowe przez okres nie dłuższy, niż jest to niezbędne.

2.6. **Integralność i poufność:** Zapewniamy odpowiednie bezpieczeństwo danych osobowych.

2.7. **Rozliczalność:** Jesteśmy w stanie wykazać przestrzeganie powyższych zasad.

3. 3. Cele i podstawy prawne przetwarzania

3.1. **Realizacja umów z klientami** - Podstawa prawna: Art. 6 ust. 1 lit. b RODO

3.2. **Marketing produktów i usług** - Podstawa prawna: Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes administratora)

3.3. **Rekrutacja pracowników** - Podstawa prawna: Art. 6 ust. 1 lit. b RODO (podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy)

4. 4. Zakres przetwarzanych danych

4.1. **Dane identyfikacyjne:** imię, nazwisko, PESEL
4.2. **Dane kontaktowe:** adres e-mail, numer telefonu, adres korespondencyjny
4.3. **Dane dotyczące zatrudnienia:** stanowisko, staż pracy, wykształcenie

5. Obowiązki pracowników

5.1. Zapoznanie się i przestrzeganie niniejszej Polityki
5.2. Uczestnictwo w szkoleniach z zakresu ochrony danych organizowanych przez firmę co najmniej raz w roku
5.3. Zgłaszanie incydentów związanych z bezpieczeństwem danych do Inspektora Ochrony Danych niezwłocznie po ich wykryciu
5.4. Stosowanie zasady "czystego biurka" i "czystego ekranu":
    i. Blokowanie komputera przy każdorazowym odejściu od stanowiska pracy
    ii. Niepozostawianie dokumentów zawierających dane osobowe na biurku po zakończeniu pracy
    iii. Przechowywanie dokumentów w zamykanych szafkach

6. Prawa osób, których dane dotyczą

6.1. Prawo dostępu do danych
6.2. Prawo do sprostowania danych
6.3. Prawo do usunięcia danych
6.4. Prawo do ograniczenia przetwarzania
6.5. Prawo do przenoszenia danych
6.6. Prawo do sprzeciwu
6.7. Procedura realizacji praw osób, których dane dotyczą:
    i. Przyjęcie wniosku (ustnego lub pisemnego) od osoby, której dane dotyczą
    ii. Weryfikacja tożsamości wnioskodawcy
    iii. Realizacja prawa lub odmowa z uzasadnieniem (w ciągu miesiąca od otrzymania żądania)
    iv. Dokumentacja podjętych działań

7. Środki bezpieczeństwa

7.1. Środki techniczne:
    i. Szyfrowanie danych przesyłanych drogą elektroniczną
    ii. Systemy firewall i antywirus na wszystkich urządzeniach firmowych
    iii. Kontrola dostępu do systemów IT poprzez indywidualne loginy i hasła
7.2. Środki organizacyjne:
    i. Regularne szkolenia pracowników z zakresu ochrony danych
    ii. Procedura nadawania i odbierania uprawnień do systemów IT

iii. Zasady korzystania z urządzeń mobilnych (np. zakaz pozostawiania urządzeń bez nadzoru w miejscach publicznych)

8. Procedury w przypadku naruszenia ochrony danych

8.1. **Identyfikacja naruszenia:** Każdy pracownik, który zauważy potencjalne naruszenie, jest zobowiązany do niezwłocznego zgłoszenia tego faktu do Inspektora Ochrony Danych.

8.2. **Zgłaszanie naruszenia wewnątrz organizacji:** IOD informuje zarząd firmy o naruszeniu w ciągu 24 godzin od jego wykrycia.

8.3. **Ocena ryzyka naruszenia:** IOD wraz z zespołem IT oceniają skalę naruszenia i potencjalne skutki dla osób, których dane dotyczą.

8.4. **Zgłaszanie naruszenia do organu nadzorczego:** W przypadku stwierdzenia ryzyka naruszenia praw i wolności osób fizycznych, IOD zgłasza naruszenie do UODO w ciągu 72 godzin od jego wykrycia.

8.5. **Zawiadamianie osób, których dane dotyczą:** Jeśli naruszenie może powodować wysokie ryzyko dla praw i wolności osób fizycznych, firma bez zbędnej zwłoki zawiadamia o tym osoby, których dane dotyczą.

8.6. **Dokumentowanie naruszeń:** IOD prowadzi rejestr wszystkich naruszeń, zawierający opis naruszenia, jego skutki oraz podjęte działania zaradcze.

9. Przekazywanie danych osobowych

9.1. **Przekazywanie danych wewnątrz UE/EOG:** Dopuszczalne na ogólnych zasadach RODO.

9.2. **Przekazywanie danych poza UE/EOG:** Możliwe tylko do krajów zapewniających odpowiedni poziom ochrony danych lub przy zastosowaniu odpowiednich zabezpieczeń (np. standardowe klauzule umowne).

9.3. **Umowy powierzenia przetwarzania danych:** Zawierane ze wszystkimi podmiotami przetwarzającymi dane w imieniu [NAZWA FIRMY] (np. dostawcy usług chmurowych, firmy kurierskie).

10. Rejestr czynności przetwarzania

10.1. **Prowadzenie rejestru:** IOD jest odpowiedzialny za prowadzenie i aktualizację rejestru czynności przetwarzania.

10.2. **Zawartość rejestru:**

i. Nazwa czynności przetwarzania
ii. Cel przetwarzania
iii. Kategorie osób i danych osobowych
iv. Kategorie odbiorców
v. Informacje o przekazywaniu danych do państw trzecich
vi. Planowane terminy usunięcia danych
vii. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

10.3. **Aktualizacja rejestru:** Rejestr jest aktualizowany przy każdej zmianie w procesach przetwarzania danych, nie rzadziej niż raz na kwartał.

11. Ocena skutków dla ochrony danych (DPIA)

11.1. **DPIA przeprowadza się w przypadku:**

i. Systematycznej, kompleksowej oceny czynników osobowych związanych z osobami fizycznymi, opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu
ii. Przetwarzania na dużą skalę szczególnych kategorii danych osobowych
iii. Systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie

11.2. **Procedura przeprowadzania DPIA:**

i. Opis planowanych operacji przetwarzania
ii. Ocena niezbędności i proporcjonalności przetwarzania
iii. Ocena ryzyka dla praw i wolności osób, których dane dotyczą
iv. Środki planowane w celu zaradzenia ryzyku

11.3. **Konsultacje z organem nadzorczym:** W przypadku wysokiego ryzyka, którego nie można zminimalizować, firma konsultuje się z UODO przed rozpoczęciem przetwarzania.

12. Inspektor Ochrony Danych (IOD)

12.1. **Dane kontaktowe IOD:** [Imię, nazwisko, email, telefon]

12.2. **Zadania i obowiązki IOD:**

i. Informowanie i doradzanie w zakresie ochrony danych
ii. Monitorowanie przestrzegania RODO i polityk ochrony danych
iii. Szkolenie personelu
iv. Przeprowadzanie audytów
v. Współpraca z organem nadzorczym

12.3. **Niezależność IOD:** IOD podlega bezpośrednio zarządowi i nie może być karany ani odwoływany za wykonywanie swoich zadań.

13. Audyty i szkolenia

13.1. Audyty:

i. **Częstotliwość:** raz w roku
ii. **Zakres:** zgodność z RODO i niniejszą polityką
iii. **Osoby odpowiedzialne:** IOD lub zewnętrzny audytor
iv. **Raportowanie:** wyniki przedstawiane zarządowi w ciągu 2 tygodni od zakończenia audytu

13.2. Szkolenia:

i. **Harmonogram:** szkolenie wstępne dla nowych pracowników, coroczne szkolenie przypominające

ii. **Tematyka:** podstawy RODO, polityka ochrony danych firmy, procedury bezpieczeństwa
iii. **Formy:** e-learning, warsztaty stacjonarne
iv. **Weryfikacja wiedzy:** test po każdym szkoleniu

13.3. **Ewaluacja i aktualizacja programów szkoleniowych:** Coroczny przegląd i aktualizacja materiałów szkoleniowych przez IOD.

14. Zarządzanie dokumentacją

14.1. **Przechowywanie dokumentacji:** W zabezpieczonym archiwum fizycznym i elektronicznym.

14.2. **Okresy retencji:**

i. Dokumenty kadrowe: 10 lat od zakończenia zatrudnienia

ii. Dokumenty księgowe: 5 lat od końca roku obrotowego

iii. Umowy: 3 lata od wygaśnięcia lub rozwiązania

14.3. **Bezpieczne niszczenie dokumentów:** Przy użyciu niszczarki lub specjalistycznej firmy zajmującej się niszczeniem dokumentów.

15. Aktualizacja polityki

15.1. **Okresowy przegląd polityki:** Raz w roku lub częściej w przypadku istotnych zmian w przepisach lub działalności firmy.

15.2. Procedura wprowadzania zmian:
i. Propozycja zmian przygotowana przez IOD
ii. Konsultacje z zarządem i działem prawnym
iii. Zatwierdzenie zmian przez zarząd
iv. Publikacja nowej wersji polityki

15.3. Informowanie pracowników o zmianach: Poprzez e-mail oraz podczas najbliższego szkolenia z zakresu ochrony danych.

Data ostatniej aktualizacji: [DATA]