

# AUDYT PROCESORA

## Zgodność przetwarzania danych ze standardem Administratora

**Procesorze**, wykonujesz operacje na danych osobowych przez nas administrowanych lub planujemy zlecić Ci usługi, w ramach których będziesz przetwarzał powierzone nam dane osobowe. Zgodnie z umową powierzenia danych osobowych, wdramy czynności kontrolne, które pozwolą nam na wykonanie audytu zgodności przetwarzania danych osobowych przez podmiot przetwarzający, z naszymi standardami ochrony danych osobowych.

Poniżej zawarliśmy pytania odnoszące się do czynności przetwarzania danych osobowych i procesów ochronnych, proszę na każde pytanie wskazać jedną z wartości:  TAK  NIE (formularz interaktywny- kliknij w kwadracik) lub zaznaczyć i opisać czemu nie zaznaczono żadnej z powyższych odpowiedzi.

Przy odpowiedzi SPEŁNIA CZĘŚCIOWO, proszę wskazać procent spełnienia warunku oraz opisać na czym polega niezgodność lub odmienny standard wykonania tego obowiązku/procesu. Można posilkować się schematem: 30%- opracowuje wdrożenie, 60%- wdrożono częściowo funkcje, 90%- w trakcie ukończenia wdrożenia. **Po przesłaniu ankiety** – w terminie 7 dni, podliczymy procent spełnienia przesłanek należytej ochrony danych osobowych w procesach przetwarzania u Ciebie w firmie. Jeżeli na podstawie tej ankiety wyjdzie, że nie spełniasz naszych standardów, lub spełniasz w stopniu niewystarczającym, przeprowadzimy poszerzony audyt procesów u Ciebie i na podstawie jego wyników rozwiążemy umowę powierzenia danych osobowych lub wskażemy jakie procesy musisz uwzględnić i standardy spełnić, żebyś mógł dalej pełnić rolę naszego procesora.

NAZWA PROCESORA: \_\_\_\_\_ ;  
NUMER NIP/PESEL: \_\_\_\_\_ ;  
WYPEŁNIŁ (IMIĘ, NAZWISKO, FUNKCJA): \_\_\_\_\_ ;  
MIEJSCOWOŚĆ: \_\_\_\_\_ , DATA: \_\_\_\_\_ ;

- 1) Czy zgodnie z RODO i umową powierzenia danych osobowych, **osoby wykonujące operacje na danych osobowych** otrzymały od procesora:
  - i) imienne upoważnienie do przetwarzania danych:  TAK  NIE
  - ii) określony zakres przetwarzanych przez te osoby danych:  TAK  NIE
  - iii) wskazanie kategorii czynności przetwarzania przez upoważnioną:  TAK  NIE
  - iv) określono termin ważności upoważnienia:  TAK  NIE
  
- 2) Czy procesor prowadzi:
  - i) rejestr kategorii czynności przetwarzania zgodny z art. 30 ust. 2 RODO, w zakresie wymaganych danych tam zawartych:  TAK  NIE
  - ii) rejestr wydanych upoważnień przetwarzania danych osobowych:  TAK  NIE
  - iii) rejestr umów powierzenia danych osobowych:  TAK  NIE
  - iv) rejestr naruszeń danych osobowych:  TAK  NIE
  
- 3) Czy podmiot przetwarzający posiada:
  - i) zatwierdzoną i opublikowaną politykę ochrony danych osobowych:  TAK  NIE
  - ii) politykę zarządzania zasobami informatycznymi:  TAK  NIE
  - iii) analizę ryzyka  TAK  NIE
  - iv) regulaminy przetwarzania danych osobowych dla personelu:  TAK  NIE
  - v) procedury w razie incydentu naruszenia danych osobowych:  TAK  NIE
  
- 4) Proszę wskazać, które z warunków procesor wykonuje:
  - i) zapoznanie pracowników i inne osoby świadczące usługi na podstawie umów cywilnoprawnych z PODO, regulaminy ochrony danych osobowych:  TAK  NIE

- ii) przeszkolenie pracowników i osób świadczących usługi na podstawie umów cywilnoprawnych z procedur ochrony danych osobowych:  TAK  NIE
- iii) cykliczne szkolenia z zakresu ochrony danych dla osób wykonujących czynności przetwarzania danych osobowych:  TAK  NIE
- iv) zawarcie z osobami przetwarzającymi dane u procesora umów poufności:  TAK  NIE
- v) audyt standardu ochrony danych osobowych przez osoby przetwarzające dane u procesora, co \_\_\_\_\_ lata:  TAK  NIE
- 5) Czy procesor stosuje:
- i) zatwierdzony kodeks postępowania- art. 40 RODO:  TAK  NIE
- ii) zatwierdzony mechanizm certyfikacji- art. 42 RODO:  TAK  NIE
- 6) Termin wykonania audytu czynności przetwarzania danych osobowych u procesora, przez niezależny podmiot:
- i) Co rok:  TAK  NIE
- ii) Co dwa lata:  TAK  NIE
- iii) Co trzy lata:  TAK  NIE
- iv) Nie wykonuje:  TAK  NIE
- 7) Procesor:
- i) weryfikuje podwykonawców w zakresie ochrony danych osobowych:  TAK  NIE
- ii) zawiera umowy powierzenia danych osobowych:  TAK  NIE
- iii) prowadzi audyt zgodności przetwarzania danych osobowych dalszych procesorów z wymogami Administratora:  TAK  NIE
- 8) Ochrona danych osobowych – zabezpieczenie lokalu procesora:
- i) czy dostęp do pomieszczeń z danymi osobowymi jest zabezpieczony przed dostępem osób trzecich:  TAK  NIE  
- proszę opisać zabezpieczenia (takie jak dostęp monitorowany, hasłowany, alarm)  
: \_\_\_\_\_
- ii) czy pomieszczenia z danymi osobowymi są ogólnodostępne w czasie godzin pracy Administratora:  TAK  NIE
- iii) budynek zewnętrzny czy jest zabezpieczony:  TAK  NIE  
- proszę opisać zabezpieczenia (takie jak dostęp monitorowany, hasłowany, alarm):  
: \_\_\_\_\_
- iv) dostęp do pomieszczeń pozostających w dyspozycji procesora, po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany:  TAK  NIE
- 9) miejsce przechowywania danych wrażliwych:
- i) czy dostęp do pomieszczeń z danymi osobowymi wrażliwymi jest zabezpieczony przed dostępem osób trzecich:  TAK  NIE  
- proszę opisać zabezpieczenia (takie jak dostęp monitorowany, hasłowany, alarm)  
: \_\_\_\_\_
- ii) czy pomieszczenia z danymi osobowymi wrażliwymi są ogólnodostępne w czasie godzin pracy Administratora:  TAK  NIE
- iii) przechowuje nośniki danych osobowych w zamkniętych szafkach/innych narzędziach/ z ograniczonym dostępem zewnętrznym:  TAK  NIE
- iv) dane wrażliwe przechowuje w pomieszczeniu z dostępem autoryzowanym:  TAK  NIE
- v) dane wrażliwe przechowuje w szafach/innych narzędziach/ zapewniających dostęp wyłącznie autoryzowany:  TAK  NIE
- 10) Czy zapewniono techniczne narzędzia oddzielające nośniki danych osobowych Administratora, od danych Procesor:  TAK  NIE

- 11) Czy zapewniono techniczne narzędzia oddzielające nośniki danych osobowych Administratora, od innych danych przetwarzanych przez Procesora:  TAK  NIE
- 12) Zabezpieczenia IT:
- i) pracownicy posiadają imienny identyfikator do systemów informatycznych:  TAK  NIE
  - ii) system zawierający dane osobowe wymusza zmianę hasel:  TAK  NIE
  - iii) zabezpieczanie nieużywanych systemów poprzez blokadę ekranu:  TAK  NIE
  - iv) oprogramowanie antywirusowe na wszystkich stacjach:  TAK  NIE
  - v) oprogramowanie posiada licencję i jest na bieżąco aktualizowane:  TAK  NIE
  - vi) szyfrowanie dysków komputerów przenośnych:  TAK  NIE
  - vii) tworzenia kopii zapasowych:  TAK  NIE
  - zakres oraz częstotliwość tworzenia kopii zapasowych: \_\_\_\_\_
  - miejsce przechowywania kopii zapasowych: \_\_\_\_\_
  - viii) procedury odtwarzania systemu po awarii oraz ich testowanie:
  - ix) korzysta z serwera własnego:  TAK  NIE
  - x) korzysta z serwera zewnętrznego zlokalizowanego w krajach o standardzie ochrony danych zgodnym z RODO:  TAK  NIE
  - xi) z serwera zewnętrznego zlokalizowanego w krajach nie spełniających standardu ochrony danych zgodnym z RODO:  TAK  NIE
  - xii) z poczty służbowej e-mail z własnej domeny:  TAK  NIE
  - xiii) z poczty służbowej e-maila z portali ogólnodostępnych:  TAK  NIE
  - xiv) korzysta z mediów społecznościowych do kontaktu z administratorami, procesorami, klientami, z przesyłaniem danych osobowych i nośników danych:  TAK  NIE
  - xv) przesyła pliki zawierające dane osobowe szyfrowane:  TAK  NIE
- 13) Procesor wdrożył procedurę:
- i) odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje niezwłocznie:  TAK  NIE
  - ii) usuwania kopii dokumentów zawierających dane osobowe z drukarek, faksów z pamięci narzędzi po wykonaniu czynności:  TAK  NIE
  - iii) połączenia imienne/narzędziowe do drukarek, faksów:  TAK  NIE
  - iv) wydawania nośników danych wrażliwych z imiennym potwierdzeniem:  TAK  NIE
  - v) odbioru nośników danych z danymi osobowymi od osób trzecich z kontrolą treści, zagrożeń, możliwości utraty danych i nośników:  TAK  NIE
  - vi) niszczenia i usuwania nośników i danych osobowych:  TAK  NIE
  - vii) procedurę anonimizacji:  TAK  NIE
- 14) Procesor:
- i) wdrożył politykę „czystego biurka”:  TAK  NIE
  - ii) wdraża nowe rozwiązania zgodnie z zasadą "privacy by design":  TAK  NIE
  - iii) działa zgodnie z zasadą "privacy by default":  TAK  NIE
- 15) Urządzenia mobilne:
- i) posiadają skonfigurowaną kontrolę dostępu:  TAK  NIE
  - ii) posiadają oprogramowania antywirusowe:  TAK  NIE
  - iii) przewidziano szybkie przywrócenie dostępności danych osobowych i dostępu do urządzeń w przypadku incydentu:  TAK  NIE
  - iv) wydano z upoważnieniem imiennym:  TAK  NIE
  - v) prowadzi się audyt wykorzystania sprzętu firmowego przez użytkownika:  TAK  NIE
  - vi) wdrożono zasady korzystania z narzędzi mobilnych dla celów prywatnych:  TAK  NIE
  - umożliwiała się instalację programów, narzędzi prywatnych na sprzęcie firmowym:  TAK  NIE
  - użytkownik loguje się do sieci niezabezpieczonych na narzędziach firmowych:  TAK  NIE

16) Ocena skutków dla ochrony danych:

- i) wykonano:  TAK  NIE
- ii) wynik oceny
  - zagrożenia o wysokim stopniu naruszenia danych występują:  TAK  NIE
  - wydano zalecenia usunięcia zagrożeń:  TAK  NIE
  - wdrożono zalecenia w organizacji:  TAK  NIE
  - wynik oceny skutków po wdrożeniu zaleceń, pozytywna:  TAK  NIE

17) Procesor:

- i) gwarantuje realizację praw osób, których dane dotyczą:  TAK  NIE
- ii) wyznaczył IOD:  TAK  NIE
- iii) wyznaczył osobę odpowiedzialną za procedury ochrony danych osobowych:  TAK  NIE
- iv) wyznaczył ASI:  TAK  NIE
- v) wyznaczył osobę odpowiedzialną za procedurę ochrony danych w zasobach informatycznych:  TAK  NIE

18) Procesor:

- i) posiada procedurę na wypadek incydentu naruszenia danych osobowych:  TAK  NIE
- ii) przeszkolił pracowników z procedury incydentu:  TAK  NIE
- iii) prowadzi monit zagrożenia wystąpienia incydentu naruszenia danych:  TAK  NIE
- iv) w ostatnim roku wystąpił incydent naruszenia danych osobowych:  TAK  NIE
  - kiedy:
  - opis incydentu:
  - stopień naruszenia danych:
  - wdrożone działania naprawcze:
  - zawiadomienie UODO:
  - zawiadomienie osób, których incydent dotyczy:

19) W ostatnim roku Procesor:

- i) miał kontrole ochrony danych przeprowadzoną przez UODO:  TAK  NIE
  - wynik kontroli:
- ii) miał kontrole ochrony danych przeprowadzoną przez podmioty trzecie:  TAK  NIE
  - wynik kontroli:
- iii) zgłosiła osoba, której dane dotyczą zgłoszenie naruszenia danych do Procesora lub innego podmiotu:  TAK  NIE
  - wynik i zasadność zgłoszenia:

Dziękujemy za wypełnienia ankiety. Jeżeli są potrzebne dodatkowe wyjaśnienia, opisy, prosimy zrobić to poniżej:

---

---

---