ANKIETA PROCESORA

Zgodność przetwarzania danych ze standardem Administratora

Szanowny Procesorze,

wykonujesz operacje na danych osobowych przez nas administrowanych lub planujemy zlecić ci usługi, w ramach których będziesz przetwarzał powierzone Ci dane osobowe. Zgodnie z umową powierzenia danych osobowych, wdrażamy 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 trzech wartości:

1- NIE SPEŁNIA, 2 – SPEŁNIA CZĘŚCIOWO, 3- SPEŁNIA

Przy odpowiedzi SPEŁNIA CZĘŚCIOWO, proszę wskazać procent spełnienia warunku oraz opisać na czym polega niezgodność lub odmienny standard wykonania tego obowiązku/procesu. Można posiłkować się schematem:
30%- opracowuje się wdrożenie, 60%- wdrożono podstawowe funkcje, 90%- w trakcie pełnego wdrożenia, nieukończone.

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:
   ii) określony zakres przetwarzanych przez te osoby danych:
   iii) wskazanie rodzaju/kategorii czynności przetwarzania przez osobę upoważnioną:
   iv) określono termin ważności upoważnienia:

2) Czy procesor prowadzi:
   i) rejestr kategorii czynności przetwarzania zgodny z art. 30 ust. 2 RODO, w zakresie wymaganych danych tam zawartych:
   ii) rejestr wydanych upoważnień przetwarzania danych osobowych:
   iii) rejestr umów powierzenia danych osobowych:
   iv) rejestr naruszeń danych osobowych:

3) Czy podmiot przetwarzający posiada:
   i) opracowaną, zatwierdzoną i opublikowaną politykę ochrony danych osobowych:
   ii) politykę zarządzania zasobami informatycznymi:
   iii) analizę ryzyka
   iv) regulaminy przetwarzania danych osobowych dla personelu:
   v) procedury w razie incydentu naruszenia danych osobowych:

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:
ii) przeszkolenie pracowników i osób świadczących usługi na podstawie umów cywilnoprawnych z procedur ochrony danych osobowych:
iii) cykliczne szkolenia z zakresu ochrony danych dla osób wykonując czynności przetwarzania danych osobowych:
iv) zawarcie z osobami przetwarzającymi dane u procesora umów poufności:
v) audyt standardu ochrony danych osobowych przez osoby przetwarzające dane u procesora, co _____ lata:

5) Czy procesor stosuje:
i) zatwierdzony kodeks postępowania- art. 40 RODO:
ii) zatwierdzony mechanizm certyfikacji- art. 42 RODO:

6) Termin wykonania audytu czynności przetwarzania danych osobowych u procesora, przez niezależny podmiot:
i) Co rok:
ii) Co dwa lata:
iii) Co trzy lata:
iv) Nie wykonuje:

7) Procesor:
i) weryfikuje podwykonawców w zakresie ochrony danych osobowych:
ii) zawiera umowy powierzenia danych osobowych:
iii) prowadzi audyt zgodności przetwarzania danych osobowych dalszych procesorów z wymogami Administratora:

8) Ochrona danych osobowych – zabezpieczenie lokalu procesora:
i) czy dostęp do pomieszczeń z danymi osobowymi jest zabezpieczony przed dostępem osób trzecich:
- proszę opisać zabezpieczenia (takie jak dostęp monitorowany, hasłowany, alarm)
ii) czy pomieszczenia z danymi osobowymi są ogólnodostępne w czasie godzin pracy Administratora:
iii) budynek zewnętrzny czy jest zabezpieczony:
- 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:

9) miejsce przechowywania danych wrażliwych:
i) czy dostęp do pomieszczeń z danymi osobowymi wrażliwymi jest zabezpieczony przed dostępem osób trzecich:
- proszę opisać zabezpieczenia (takie jak dostęp monitorowany, hasłowany, alarm)
ii) czy pomieszczenia z danymi osobowymi wrażliwymi są ogólnodostępne w czasie godzin pracy Administratora:
iii) przechowuje nośniki danych osobowych w zamkniętych szafkach/innych narzędziach/ z ograniczonym dostępem zewnętrznym:
iv) dane wrażliwe przechowuje w pomieszczeniu zapewniającym dostęp autoryzowany:
v) dane wrażliwe przechowuje w szafach/innych narzędziach/ zapewniających dostęp wyłącznie autoryzowany:

10) Czy zapewniono techniczne narzędzia oddzielające nośniki danych osobowych Administratora, od danych Procesor:

11) Czy zapewniono techniczne narzędzia oddzielające nośniki danych osobowych Administratora, od innych danych przetwarzanych przez Procesora:

12) Zabezpieczenia IT:
i) pracownicy posiadają imienny identyfikator do systemów informatycznych:
ii) system zawierający dane osobowe wymusza zmianę haseł:
iii) zabezpieczanie nieużywanych systemów poprzez blokadę ekranu lub w inny sposób:
iv) oprogramowanie antywirusowe na wszystkich stacjach:
v) oprogramowanie posiada licencję i jest na bieżąco aktualizowane:
vi) szyfrowanie dysków komputerów przenośnych:
vii) tworzenia kopii zapasowych:
- zakres oraz częstotliwość tworzenia kopii zapasowych:
- miejsce przechowywania kopii zapasowych:
viii) procedury odtwarzania systemu po awarii oraz ich testowanie:
ix) korzysta z serwera własnego:
x) korzysta z serwera zewnętrznego zlokalizowanego w krajach o standardzie ochrony danych zgodnym z RODO:
xi) z serwera zewnętrznego zlokalizowanego w krajach nie spełniających standardu ochrony danych zgodnym z RODO:
xii) z poczty służbowej e-mail z własnej domeny:
xiii) z poczty służbowej e-maila z portali ogólnodostępnych:
xiv) korzysta z mediów społecznościowych do kontaktu z administratorami, procesorami, klientami, z przesyłaniem danych osobowych i nośników danych:
xv) przesyła pliki zawierające dane osobowe szyfrowane:

13) Procesor wdrożył procedurę:
i) odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje niezwłocznie:
ii) usuwanie kopii dokumentów zawierających dane osobowe z drukarek, faksów z pamięci narzędzi po wykonaniu czynności:
iii) połączenia imienne/narzędziowe do drukarek, faksów:
iv) wydawania nośników danych wrażliwych z imiennym potwierdzeniem:
v) odbioru nośników danych z danymi osobowymi od osób trzecich z kontrolą treści, zagrożeń, możliwości utraty danych i nośników:
vi) niszczenia i usuwania nośników i danych osobowych:
vii) procedurę anonimizacji:

14) Procesor:
i) wdrożył politykę „czystego biurka”:
ii) wdraża nowe rozwiązania zgodnie z zasadą "privacy by design":
iii) działa zgodnie z zasadą "privacy by default":

15) Urządzenia mobilne:
i) posiadają skonfigurowaną kontrolę dostępu:
ii) posiadają oprogramowania antywirusowe:
iii) przewidziano szybkie przywrócenie dostępności danych osobowych i dostępu do urządzeń w przypadku incydentu:
iv) wydano z upoważnieniem imiennym:
v) prowadzi się audyt wykorzystania sprzętu firmowego przez użytkownika:
vi) wdrożono zasady korzystania z narzędzi mobilnych dla celów prywatnych:
- umożliwia się instalację programów, narzędzi prywatnych na sprzęcie firmowym:
- użytkownik może logować się do sieci zewnętrznych internetowych na narzędziach firmowych:

16) Ocena skutków dla ochrony danych:
i) wykonano:
ii) wynik oceny
- zagrożenia o wysokim stopniu naruszenia danych występują:

- wydano zalecenia usunięcia zagrożeń:
- wdrożono zalecenia w organizacji:
- wynik oceny skutków po wdrożeniu zaleceń w zakresie zagrożeń o wysokim stopniu naruszenia:

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

18) Procesor:
   i) posiada procedurę na wypadek incydentu naruszenia danych osobowych:
   ii) przeszkolił pracowników z procedury incydentu:
   iii) prowadzi monit zagrożenia wystąpienia incydentu naruszenia danych:
   iv) w ostatnim roku wystąpił incydent naruszenia danych osobowych:
   - 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:
   - wynik kontroli:
   ii) miał kontrole ochrony danych przeprowadzoną przez podmioty trzecie:
   - wynik kontroli:
   iii) zgłosiła osoba, której dane dotyczą zgłoszenie naruszenia danych do Procesora lub innego podmiotu:
   - wynik i zasadność zgłoszenia:

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

_____

_____

_____