

Warszawa, 21.05.2025 r.

Jak przygotować się do kontroli UODO? Praktyczny przewodnik dla Twojej firmy

Publikacja planu kontroli sektorowych na 2025 rok, opisana we wcześniejszym [artykule](#), bez wątpienia skłania do refleksji – nie tylko nad tym, czy nasza organizacja może znaleźć się na liście podmiotów wytypowanych do kontroli (a doświadczenie pokazuje, że może), ale przede wszystkim: czy jesteśmy na taką kontrolę gotowi?

Choć sama zapowiedź wizyty Urzędu Ochrony Danych Osobowych potrafi wywołać niepokój, warto pamiętać, iż nie oznacza ona automatycznie występowania nieprawidłowości w naszej organizacji. Może być szansą na wykazanie, że nasz system ochrony danych osobowych działa prawidłowo, a obowiązki wynikające z RODO są realizowane w sposób zgodny z prawem i dobrą praktyką. Kluczem do pozytywnego przebiegu kontroli jest jednak odpowiednie przygotowanie – nie tylko dokumentacyjne, ale również organizacyjne i komunikacyjne.

Rodzaje kontroli i ich podstawa prawna

Prezes Urzędu Ochrony Danych Osobowych przeprowadza kontrole na podstawie art. 78 ustawy o ochronie danych osobowych. Dotyczą one dotycząca zgodności przetwarzania danych osobowych z przepisami RODO oraz ustawą krajową. Kontrole dzielą się na planowe (zgodne z rocznym planem kontroli) oraz doraźne – przeprowadzane w wyniku skargi, naruszenia lub w ramach bieżącego monitorowania przestrzegania przepisów.

Kontrola może obejmować:

- ocenę wdrożenia odpowiednich środków technicznych i organizacyjnych, stosowanych w celu przetwarzania danych osobowych,
- zgodność przetwarzania z RODO, ustawą o ochronie danych osobowych oraz z uwzględnieniem: charakteru, zakresu, kontekstu, celów przetwarzania i ryzyka naruszenia praw i wolności,
- sprawdzenie, czy stosowane środki techniczne i organizacyjne są poddawane regularnym przeglądom i uaktualnieniom.

Jak przygotować się do kontroli?

Zacznijmy od formalności – organizacja musi pisemnie wskazać osobę upoważnioną do reprezentowania jej w trakcie kontroli (jeśli nie będzie to osoba zarządzająca). Warto z wyprzedzeniem wyznaczyć pracownika, który będzie dostępny przez cały czas trwania kontroli i wyposażony w odpowiednie upoważnienie.

Pismo informujące o kontroli zawiera jej zakres – na tej podstawie należy przygotować stosowną dokumentację i zapewnić dostępność osób posiadających wiedzę w zakresie objętym kontrolą (np. administrator systemu, właściciel biznesowy, użytkownicy).

Niezbędna dokumentacja może obejmować:

- strukturę organizacyjną,
- informację o wyznaczeniu IOD,
- rejestr czynności przetwarzania (RCP) / rejestr kategorii czynności przetwarzania (RKCP) dokonywanych w imieniu administratora,
- procedury ochrony danych obowiązujące w organizacji,
- inne procedury wewnętrzne dotyczące badanego procesu,
- dokumentowanie naruszeń,
- oceny ryzyka,

- testy równowagi (prawnie uzasadnionego interesu),
- klauzule zgód i obowiązki informacyjne,
- umowy powierzenia przetwarzania danych,
- inne informacje o miejscach przechowywania danych, sposobach ich zabezpieczeń (np. o kopiach zapasowych, o wdrożeniu środków kryptograficznych),
- informacje o regularnych przeglądach i uaktualnieniach (monitorowanie bezpieczeństwa systemów, przeprowadzanie okresowych testów bezpieczeństwa, aktualizacje).

Powyższa lista dokumentów do przygotowania nie jest katalogiem zamkniętym! Zależy przede wszystkim od przedmiotu kontroli – w niektórych przypadkach Pracownicy UODO nie będą potrzebowali całego RCP, a np. jedynie wycinek dotyczący zakresu kontroli. Podobnie z procedurami: w kręgu zainteresowania nie będą absolutnie wszystkie regulacje obowiązujące w organizacji, a jedynie te dokumenty, które dotyczą sprawy.

W celu uniknięcia paniki, problemów z drukarkami (które lubią odmawiać współpracy, gdy są najbardziej potrzebne), warto wcześniej przygotować kserokopie dokumentów, o które mogą poprosić kontrolujący. Jeżeli samodzielnie nie jesteśmy w stanie określić, jakie to mogą być dokumenty – pytajmy. Zadzwońmy do UODO, spróbujmy nawiązać bezpośredni kontakt i ustalić, które dokumenty będą niezbędne. Oszczędzi to stresu, czasu spędzonego na staniu przy drukarkach, pokaże również nasze odpowiednie przygotowanie i zaangażowanie w sprawne przeprowadzenie kontroli. Dokumenty lub wydruki, które przekazujemy kontrolującym, powinny być poświadczane za zgodność z oryginałem.

Co zapewnić organizacyjnie?

Poza przygotowaniem merytorycznym to na nas jako na kontrolowanych, ciąży obowiązek zapewnienia pracownikom Urzędu odpowiednich warunków organizacyjnych do przeprowadzenia kontroli. Jeżeli dysponujemy zasobami lokalowymi, warto zarezerwować na czas całej kontroli salę konferencyjną lub pokój do wyłącznej dyspozycji kontrolujących. Jest to miejsce, w którym kontrolujący będą prowadzić rozmowy z pracownikami składającymi wyjaśnienia, naradzać się i sporządzać protokoły przesłuchań lub z kontroli. O ile kontrolujący zazwyczaj dysponują własnym sprzętem, należy zapewnić papier do drukarki oraz samodzielnie sporządzać kopie dokumentów lub wydruków, o które zostaniemy poproszeni.

Powyższe nie jest wyłącznie przejawem naszej dobrej woli, a obowiązkiem wynikającym z ustawy o ochronie danych osobowych. Zgodnie z art. 84 ust. 2 i 3 ustawy, *kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach.*

Jak przebiega kontrola?

Nadeszła godzina zero – kontrolujący pojawiają się w naszej organizacji. Każda kontrola zaczyna się od wymiany upoważnień – kontrolujący okazują swoje pisemne upoważnienie wraz z legitymacją służbową, jednocześnie otrzymując upoważnienie osoby reprezentującej spółkę w trakcie kontroli.

Upoważnienie kontrolujących zawiera m.in.:

- podstawę prawną przeprowadzenia kontroli,
- dane osób przeprowadzających kontrolę,
- zakres przedmiotowy kontroli,
- czas jej trwania,
- podpis Prezesa Urzędu Ochrony Danych Osobowych.

Pamiętajmy, iż kontrolujący nie posiadają pełnej wiedzy o naszej organizacji i pierwsze rozmowy powinny polegać na „onboardingu”, przedstawieniu w ogólnym zarysie czym się zajmujemy, jak jest zbudowana nasza organizacja (tu przydatne będzie pokazanie struktury organizacyjnej), jakie dane osobowe przetwarzamy, w jakim celu, na jakiej podstawie prawnej, z jakiego źródła, przez jaki czas je przechowujemy (najwygodniej wspomóc się RCP), jak spełniamy obowiązki informacyjne, czy wszystkie osoby działają z upoważnienia.

Kontrolujący w trakcie kontroli mają prawo m.in. do:

- wstępu do budynków i pomieszczeń (w godzinach 6:00-22:00).
- wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli.
- przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych.
- żądania złożenia pisemnych lub ustnych wyjaśnień
- przesłuchiwania w charakterze świadka osoby, w zakresie niezbędnym do ustalenia stanu faktycznego.

Pamiętajmy, iż kontrolujący są obowiązani do zachowania w tajemnicy informacji, o których dowiedzieli się w toku prowadzonych prac.

Kontrolujący ustalają stan faktyczny na podstawie otrzymanych lub zebranych dowodów, w szczególności: dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg czynności kontrolnych oraz ustalenia przedstawia się w protokole kontroli, który następnie jest przekazywany kontrolowanej organizacji. Kontrolowany w terminie 7 dni od dnia przedstawienia protokołu kontroli do podpisu podpisuje go albo składa pisemne zastrzeżenia do jego treści. Pamiętajmy, iż mamy pełne prawo do zgłaszania poprawek, składania dodatkowych wyjaśnień, jeżeli w naszej ocenie temat nie został wyczerpany. W naszym interesie jest jak najdokładniejsze wyjaśnienie sprawy i ukazanie, w jaki sposób organizacja dba o bezpieczne przetwarzanie danych osobowych.

Podsumowanie

Kontrola Prezesa UODO nie musi oznaczać negatywnych konsekwencji dla podmiotu kontrolowanego. Urząd, prowadząc kontrole, nie dąży wyłącznie do wymierzania sankcji – celem jest także edukacja, prewencja i wspieranie administratorów w prawidłowym stosowaniu przepisów RODO. Kluczem do pozytywnego przebiegu kontroli jest rzetelne przygotowanie, przejrzysta dokumentacja i gotowość do współpracy.

Utrudnianie działań kontrolnych, uniemożliwianie wstępu na teren obiektów czy odmowa udostępnienia dokumentów nie pomoże nam uniknąć konsekwencji, a wręcz przeciwnie – jest karane. Dlatego bardzo istotna jest otwartość i przekazywanie informacji. Gdyby jednak otrzymali Państwo informację z Urzędu o planowanej kontroli i nadal czuli niepokój – jesteśmy gotowi zapewnić nasze wsparcie w przygotowaniu Państwa organizacji do kontroli oraz przeprowadzeniu przez ten proces – korzystając z naszego bezpośredniego doświadczenia w tym obszarze.

Marcin Stryzko – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.