Jak przygotować się do kontroli UODO?

Im więcej danych osobowych przetwarzasz i im większa jest Twoja organizacja, tym bardziej prawdopodobne, że ktoś sprawdzi Twoją zgodność z RODO. Ten artykuł pomoże Ci się dobrze przygotować do kontroli Prezesa Urzędu Ochrony Danych Osobowych. Nasze porady będą dotyczyły przede wszystkim kontroli UODO. Jeśli jednak dobrze się na nią przygotujesz, to poradzisz sobie również z kontrolą zewnętrznych audytorów.

Dlaczego kontroluje mnie Urząd Ochrony Danych Osobowych?

Źródła kontroli UODO mogą być trzy. **Pierwszy przypadek** to rutynowa kontrola branży w której działasz (tzw. **kontrola planowa**). Co roku w styczniu Prezes UODO ogłasza plan kontroli sektorowych, na podstawie którego podmioty z określonych sektorów oraz branż mogą oczekiwać u siebie wizyty inspektorów. Zgodnie z treścią planu kontroli sektorowych UODO na 2020 r., szczególny nacisk położono na badanie stanu przestrzegania przepisów w bankach oraz podmiotach korzystających z systemu zdalnego odczytu wodomierzy. Warto wskazać, że Prezes UODO z powodu stanu epidemii COVID-19 nie opracował planu kontroli sektorowych na rok 2021, zaś plan ma zostać sporządzony wtedy, gdy sytuacja epidemiczna pozwoli na bezpieczne przeprowadzenie kontroli.

Drugie źródło kontroli to skargi na Twoją organizację. Mogą one wpłynąć od osób, których dane osobowe przetwarzasz, sygnalistów lub z inicjatywy innych organów, którym przepisy nadają uprawnienia kontrolne, sądów i prokuratur. Stosowne informacje mogą również zostać pozyskane przez UODO z mediów, chociażby w zakresie podejrzenia dużego wycieku danych osobowych. Jeśli ktoś złożył na Ciebie skargę, to osobista kontrola w Twojej organizacji, zwłaszcza w obecnym stanie związanym z epidemią, będzie jednak ostatecznością. Najpierw inspektorzy spróbują wyjaśnić sprawę korespondencyjnie.

Trzecim źródłem kontroli może być incydent ochrony danych osobowych zgłoszony przez Ciebie lub organizację, z którą współpracujesz. W przypadkach wyjątkowo poważnych i źle zaraportowanych incydentów, UODO nie wyjaśnia sprawy korespondencyjnie. Może od razu wszcząć kontrolę w Twojej siedzibie.

W drugim i trzecim przypadku mamy do czynienia z tzw. **kontrolą doraźną**, przeprowadzaną na podstawie uzyskanych przez Prezesa UODO informacji.

Ostatnim, **czwartym ze źródeł** kontroli może być sam Prezes UODO. Dobór podmiotów do tzw. **kontroli wyrywkowej** następuje zgodnie ze swobodnym wyborem organu. Jest ona przeprowadzana w ramach spoczywającego na UODO obowiązku monitorowania przestrzegania stosowania przepisów RODO.

Czy może mnie kontrolować ktoś inny niż UODO?

W tym przypadku również może być kilka źródeł kontroli. **Po pierwsze**, może być to kontrola prowadzona przez centralę. Spółka matka chce wiedzieć czy w spółce córce prawidłowo wdrożono procedury RODO. Podobnie może wyglądać sytuacja w sektorze publicznym. Jakiś czas temu, pomagaliśmy na przykład klientowi, który był jednostką podległą burmistrzowi miasta. Burmistrz postanowił skontrolować podległe mu jednostki pod kątem wdrożenia procedur RODO.

Po drugie, jeśli przetwarzasz powierzone dane osobowe, to możesz spodziewać się kontroli przygotowanej przez administratora danych. Na przykład, jeśli udostępniasz klientom system informatyczny, który przetwarza dane osobowe, to musisz liczyć się z tym, że Twoi klienci mogą chcieć sprawdzić poziom Twojego wdrożenia. Kontrola jest praktycznie przesądzona, jeśli po Twojej stronie nastąpił wyciek danych lub inny incydent, w wyniku którego Twoi klienci stracili cenne dane.

Ile mam czasu zanim się pojawią i ile potrwa sama kontrola?

Czas trwania kontroli będzie zależał od kontrolującego. Jeśli kontroluje Cię Urząd Ochrony Danych Osobowych, to zgodnie z art. 89 Ustawy o ochronie danych osobowych, kontrola może trwać **do 30 dni**. Oczywiście nie oznacza to, że inspektorzy ten czas spędzą u Ciebie. W praktyce, kontrola na miejscu zajmuje około tygodnia. Reszta działań, jak np. weryfikacja dostarczonych w toku kontroli dokumentów i złożonych wyjaśnień, odbywa się poza naszą organizacją.

W całej naszej praktyce zawodowej, nigdy nie spotkaliśmy się z niezapowiedzianą kontrolą. Inspektorzy zawsze zapowiadają swoje przybycie z wyprzedzeniem. Im również zależy na tym, żeby w dniu kontroli obecny był IOD czy inna osoba odpowiedzialna za obszar RODO. Teoretycznie jednak, inspektorzy mogą pojawić się również niezapowiedziani.

Jeśli chodzi o kontrole prowadzone przez inne podmioty (np. administratora danych, audytorów zewnętrznych), sprawa ma się bardzo podobnie jak z kontrolami UODO. Również najczęściej są zapowiadane. Sam czas pierwszego etapu kontroli, w który jesteśmy zaangażowani. znacząco się jednak skraca. To już nie tydzień, a zazwyczaj kilka dni. Również forma kontroli często jest inna. Tutaj obecnie przeważa forma zdalna, za pośrednictwem video.

Zanim wpuścisz obce osoby do Twojej organizacji

Inspektorzy UODO posiadają legitymacje służbowe i powinni przedstawić imienne upoważnienie do przeprowadzenia kontroli. Ponieważ zdarzały się już przypadki podszywania się pod inspektorów UODO (o czym pisał sam UODO), to rekomenduję dobrze sprawdzić te kwestie formalne. Również w przypadku audytorów zewnętrznych dochowaj należytej staranności przy identyfikowaniu gości. Pamiętaj, że będą mieli dostęp do wielu poufnych informacji za których bezpieczeństwo odpowiada Twoja organizacja.

Co na pewno będzie sprawdzane?

Jest kilka elementów, które stanowią standardowy element każdej kontroli. Niezależnie od tego czy jest to kontrola UODO czy audyt zewnętrzny przygotuj się na sprawdzenie:

1) **RCP i RKCP**. Oba rejestry są fundamentem systemu ochrony danych osobowych. Kontrolerzy sprawdzą na pewno czy je posiadasz. W większości przypadków sprawdzą również, kiedy były ostatni raz aktualizowane.

2) **Procedury RODO**. Kluczowe procedury to między innymi: raportowanie incydentów, privacy by design / default, ocena ryzyka, nadawanie upoważnień, realizacja praw osób. W większości przypadków te procedury znajdują się w jednym dokumencie tj. Polityce ochrony danych osobowych.

3) **Raporty z audytów**. Wdrożenie dokumentacji i prowadzenie RCP czy RKPC powinno opierać się na uprzednim zebraniu informacji, zazwyczaj w formie audytu. Inspektorzy na pewno poproszą Cię o wskazanie źródła obowiązujących procedur oraz będą chcieli wiedzieć czy systematycznie kontrolujesz swoją zgodność z przepisami oraz wdrożonymi zasadami. Zapytają również o to, kiedy prowadzony był ostatni audyt i poproszą o raport.

4) **Ocena ryzyka**. Zasada podejścia opartego na ryzyku (ang. risk-based approach) stanowi kluczowy element RODO. Inspektorzy sprawdzą czy dokonałeś analizy charakteru, zakresu, kontekstu i celów przetwarzania danych w odniesieniu do ryzyka naruszenia praw i wolności osób, których dane dotyczą.

5) **Rejestr incydentów**. To kolejny stały element każdej kontroli. Tutaj co może Cię zaskoczyć, pusty rejestr niekoniecznie będzie odebrany pozytywnie. Jeśli przez kilka lat nie było żadnego incydentu, inspektorzy mogą to uznać za podejrzane.

6) **Klauzule zgód i obowiązki informacyjne**. Inspektorzy poproszą Cię o stosowne treści klauzul dla każdego ze zmapowanych procesów. Sprawdzą również mechanizm pozyskiwania zgód i ich wycofywania.

7) **Obszar IT security**. Na pewno będzie sprawdzany przez inspektorów UODO. Kontrole zewnętrzne już nie zawsze sprawdzają poziom zabezpieczeń IT. Polecamy tutaj np. nasz artykuł o cyberbezpieczeństwie według ENISA.

Żeby pomóc Ci sprawdzić stopień Twojej gotowości do kontroli, przygotowaliśmy krótką checklistę kontrolną do pobrania.

Pobierz checklistę kontrolną pomagającą przygotować się do inspekcji UODO

POBIERZ

Zadbaj również o Zespół

Twój zespół również będzie kontrolowany. Przygotuj pracowników i przypomnij najważniejsze kwestie. O samym szkoleniu zespołu dużo pisaliśmy na łamach naszego bloga. Inspektorzy sprawdzą, czy pracownicy posiadają upoważnienia do przetwarzania danych osobowych. Sprawdzone będzie również to czy zostali przeszkoleni z zakresu RODO. Przygotuj zatem upoważnienia i dowody na to, że zostali poddani treningowi. Mogą to być elektroniczne potwierdzenia obecności na szkoleniu, listy obecności etc.

Wsparcie przy przygotowaniu pisma do UODO

Otrzymałeś/aś pismo od UODO i nie wiesz jak na nie odpowiedzieć? Obawiasz się konsekwencji związanych z błędnym opisem stanu faktycznego i prawnego? Daj sobie pomóc i skorzystaj z pomocy ekspertów, którzy brali udział w kontrolach GIODO/UODO oraz udzielali odpowiedzi na kilkadziesiąt pism od polskiego regulatora.

Koszt konsultacji: 300 zł netto / h.

Wypełnij poniższy formularz i zgłoś potrzebę konsultacji przy przygotowaniu pisma do UODO (dyżurujemy również w weekendy, odpowiemy w ciągu maksymalnie 2 godzin).

FORMULARZ

Poznaj procedury w ramach których działają inspektorzy UODO

Jeśli Twoja kontrola jest realizowana przez UODO, to sam proces kontroli jest regulowany przez Ustawę o ochronie danych osobowych. Art. 84 uodo daje inspektorom szerokie uprawnienia, w tym m.in.:

- wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń – kontrolujący na szczęście to też ludzie i zarówno zaczynają, jak i kończą dzień pracy zgodnie z godzinami pracy w kontrolowanej jednostce,
- wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli – kontrolowany sporządza we własnym zakresie kopie i wydruki dokumentów, o jakie poproszą kontrolujący i potwierdza za zgodność z oryginałem,
- przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych – oznacza to, że inspektorzy mogą oglądać pomieszczenia, gdzie są przetwarzane dane osobowe, sprawdzić czy pomieszczenia i szafy są zamykane na klucz, czy jest system alarmowy, monitoring wizyjny, jak ustawione są monitory komputerów, itp.,
- żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego – za pracownika kontrolowanego uznaje się osobę zatrudnioną na podstawie stosunku pracy lub wykonującą pracę na podstawie umowy cywilnoprawnej,
- zlecania sporządzania ekspertyz i opinii,
- w uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub dźwięk – informatyczne nośniki danych na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.

Jeśli nie wpuścisz kontrolujących do swojej organizacji, to pamiętaj, że Prezes UODO lub kontrolujący mogą zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli będzie to niezbędne do wykonywania czynności kontrolnych.

Na koniec kontroli, otrzymasz do podpisania jej protokół. Masz 7 dni od momentu przedstawienia protokołu na jego podpisanie lub złożenie pisemnych zastrzeżeń do jego treści.

W przypadku złożenia zastrzeżeń, kontrolujący dokonuje ich analizy i w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.

W razie nieuwzględnienia zastrzeżeń w całości albo części otrzymasz informacje o tym wraz z uzasadnieniem.

Uwaga! Brak doręczenia kontrolującemu podpisanego protokołu kontroli i niezgłoszenie zastrzeżeń we wskazanym terminie, uznaję się za odmowę podpisania protokołu kontroli.

Przygotuj się mentalnie do kontroli

Bycie kontrolowanym nie jest nigdy przyjemne. Zapewnij sobie wsparcie w zespole. Wygospodaruj czas, żeby bieżące projekty nie dekoncentrowały Twojej uwagi. Koniecznie przygotuj wszystkie dokumenty, zwłaszcza te o których pisałem w poprzedniej części tekstu.

Pamiętaj o tym, że Twoje nastawienie do kontrolujących też ma znaczenie. Im bardziej widać po Tobie napięcie i stres, tym bardziej kontrolujący będą zastanawiali się czy kryje się za nimi coś więcej niż naturalne przejęcie sytuacją.

Zdarza się, że kontrolujący są wyjątkowo skrupulatni i świadomie bądź nieświadomie będą próbowali nas wyprowadzić z równowagi. Na tego typu trudne przypadki, mamy bardzo pomocne rozwiązanie, o którym opowiemy w najnowszym odcinku Czasu na RODO.

Podsumowanie

Jeśli Twój system ochrony danych osobowych, jest na bieżąco monitorowany, a RODO zostało realnie wdrożone, nie masz się czego obawiać. Jeśli jednak masz wątpliwości czy obawy, skontaktuj się z nami. Pomożemy Ci w trybie pilnym przygotować się do kontroli UODO.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist sp. z o.o.

Źródła:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych)
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych