Kontrola: jak ustrzec się kosztownych błędów

Postępowanie w sprawie naruszeń przepisów o ochronie danych osobowych składa się zwykle z trzech etapów. Pierwszym jest kontrola, podczas której kontrolerzy UODO zbierają dowody w celu oceny, czy do naruszenia faktycznie doszło. W razie takiego właśnie ustalenia – rozpoczyna się drugi etap, tj. postępowanie przed PUODO.

PUODO przeprowadza postępowanie na podstawie przepisów Kodeksu postępowania administracyjnego ze zmianami wprowadzonymi ustawą o ochronie danych osobowych. Etap ten kończy się wydaniem decyzji. Jeżeli jest ona negatywna przedsiębiorca może się od niej odwołać. Rozpocznie się wówczas trzeci etap, tj. postępowanie sądowo-administracyjne.

Organ nadzoru przeprowadził 100 kontroli od maja 2018r. do czerwca 2019r.

ETAP I. KONTROLA

Kontrolą może być objęty każdy, kto prowadzi działalność związaną z przetwarzaniem danych osobowych.

Wyróżnia się trzy rodzaje kontroli:

1) prowadzona zgodnie z zatwierdzonym przez PUODO planem kontroli,
2) prowadzona na podstawie uzyskania przez UODO informacji (skargi, zawiadomienia) o potencjalnych naruszeniach przepisów przez dany podmiot,
3) prowadzona w ramach bieżącego monitorowania przez PUODO przestrzegania przepisów przez przedsiębiorców oraz inne jednostki.

SEKTORY SPRAWDZANE W 2019 R.

Zgodnie z ustalonym planem kontroli sektorowych na rok 2019, UODO planowało objąć szczególnym nadzorem następujące branże:

- telemarketingową,
- brokerów danych – w zakresie podstaw prawnych przetwarzania danych, oraz
- sektor bankowy i ubezpieczeniowy – w zakresie profilowania.

Podmioty prowadzące działalność w tych sektorach powinny być zatem szczególnie przygotowane na możliwość przeprowadzenia w najbliższym czasie kontroli RODO. Należy jednak mieć świadomość, że – niezależnie od powyższych uwag – kontrole mogą dotyczyć także każdej innej branży.

Konieczna zapowiedź

Ustawa o ochronie danych osobowych nie wspomina nic na temat tego, czy kontrole UODO muszą być zapowiadane. Konieczne jest zatem zastosowanie przepisów ogólnych, tj. ustawy Prawo przedsiębiorców. Stanowią one w przepisie art. 48 ust. 1, że organ kontroli zawiadamia przedsiębiorcę o zamiarze wszczęcia kontroli.

Można się jednak spotkać z poglądem, że kontrole ws. RODO mogą być niezapowiedziane. Takie stanowisko prezentuje również UODO. Pracownicy Urzędu informują przedsiębiorców, że kontrole sektorowe są niezapowiadane, natomiast zapowiadane są kontrole wszczynane na podstawie wniesionej skargi. Czy takie podejście organu i niezawiadamianie o kontrolach sektorowych jest słuszne i zgodne z przepisami?

Prawo przedsiębiorców określa przypadki, kiedy nie jest konieczne zawiadamianie o kontroli (por. art. 48 ust. 11). Możliwość dokonania kontroli RODO bez zawiadomienia nie została jednak wprost wskazana w tym przepisie. Jednocześnie, wyłączenie obowiązku zawiadamiania o kontroli dotyczy m.in. przypadku, gdy kontrola ma zostać przeprowadzona na podstawie bezpośrednio stosowanych przepisów prawa Unii Europejskiej. Czy to oznacza, że kontrola z zakresu ochrony danych osobowych podlega wyłączeniu spod obowiązku zawiadamiania z uwagi na to, że RODO jest rozporządzeniem unijnym bezpośrednio stosowanym w Polsce?

W naszej ocenie takie stanowisko jest błędne. Kontrola UODO odbywa się bowiem faktycznie na podstawie przepisów krajowych. Dotyczy ona, co prawda, stosowania przepisów unijnych, ale jest prowadzona na podstawie m.in. przepisów polskiej ustawy o ochronie danych osobowych, nie zaś bezpośrednio na podstawie RODO. Konieczne jest zatem zawiadomienie o kontroli.

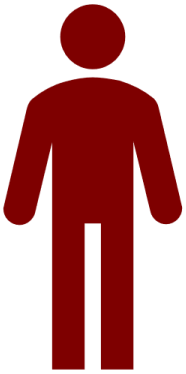
Uprawnienia i obowiązki

Kontrolerzy posiadają szereg uprawnień, które zostały określone w przepisach krajowej ustawy o ochronie danych osobowych. Uprawnienia kontrolerów wpływają na zakres obowiązków przedsiębiorcy w związku z prowadzoną kontrolą – patrz ramka.

Uprawnienia / obowiązki kontrolującego i kontrolowanego

Uprawnienia kontrolera

- wstęp na teren przedsiębiorstwa (grunt, budynki, lokale i pomieszczenia) w godzinach od 6:00 do 22:00
- wglądu do dokumentów i informacji
- przeprowadzanie oględzin miejsc, przedmiotów, urządzeń
- weryfikacja systemów informatycznych i nośników danych
- żądanie złożenia pisemnych lub ustnych wyjaśnień
- przesłuchiwanie w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego
- zlecanie sporządzania ekspertyz i opinii.
- utrwalanie przebiegu kontroli przy pomocy urządzeń rejestrujących obraz lub dźwięk (w uzasadnionych przypadkach)
- żądanie tłumaczenia dokumentacji na język polski



Obowiązki kontrolowanego

- zapewnienie kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunków i środki niezbędne do sprawnego przeprowadzenia kontroli,
- sporządzenie we własnym zakresie kopii lub wydruków dokumentów
- sporządzenie we własnym zakresie kopii oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach
- potwierdzanie za zgodność z oryginałem sporządzonych kopii lub wydruków
- umożliwienie przesłuchania pracowników w charakterze świadka
- przetłumaczenia dokumentacji na język polski

Podsumowanie w protokole

Po przeprowadzeniu kontroli sporządzany jest protokół w oparciu o zebrane dowody. Zawiera on:
- zakres podejmowanych czynności kontrolnych,
- osoby, które brały udział w kontroli,
- opis stanu faktycznego ustalonego w toku kontroli,
- inne informacje mające kluczowe znaczenie w aspekcie oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

W protokole muszą się również znaleźć pouczenia kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu kontroli oraz o prawie odmowy jego podpisania.
Podpisany przez kontrolującego protokół jest przekazywany podmiotowi kontrolowanemu, który w terminie 7 dni powinien go podpisać albo wnieść zastrzeżenia. Kontrolujący może uwzględnić zastrzeżenia. Jeśli ich nie uzna – ma obowiązek uzasadnić swoje stanowisko i przekazać stosowne informacje w tym zakresie.

ETAP II. Postępowanie przez PUODO
Jeśli nie doszło do naruszenia przepisów, kontrolowany otrzyma stosowną informację od organu nadzoru. Na tym jego udział w postępowaniu się kończy.

Jeżeli natomiast w trakcie kontroli stwierdzono, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, wszczynane jest postępowanie, prowadzone przez Prezesa UODO. Z tym momentem otwiera się etap drugi – postępowania administracyjnego przez PUODO. Zastosowanie tu mają przepisy Kodeksu postępowania administracyjnego, w szczególności w zakresie konieczności zawiadomienia o wszczęciu postępowania przed PUODO.

Co istotne dla wielu przedsiębiorców, PUODO – jeszcze przed wydaniem decyzji – może wydać postanowienie w przedmiocie ograniczenia przetwarzania danych osobowych, które są objęte postępowaniem. Takie uprawnienie PUODO może się wiązać z wystąpieniem wielu negatywnych skutków dla przedsiębiorcy.

Przykład
Przedmiotem postępowania są bazy marketingowe. Dane znajdujące się w tych bazach agencja marketingowa wykorzystuje codziennie w prowadzonej działalności. Ograniczenie możliwości przetwarzania tych danych spowodowałby faktyczny brak możliwości prowadzenia działalności przez przedsiębiorcę i znaczne ograniczenie przychodów.

Decyzja kończąca sprawę
Etap postępowania administracyjnego zamyka wydanie przez PUODO decyzji. Decyzja kończąca sprawę powinna zostać wydana z uwzględnieniem zasad określonych w przepisach Kodeksu postępowania administracyjnego. Jaką decyzję może wydać PUODO?

Jeżeli firma w trakcie prowadzonego postępowania usunęła w całości stwierdzone uchybienia, organ najpewniej wyda decyzję umarzającą postępowanie. Jeśli uchybienia nadal istnieją, Urząd nakaże określone rozwiązanie, które może polegać np. na:
- spełnieniu żądania osoby, której dane dotyczą,
- wprowadzeniu czasowego lub całkowitego ograniczenia przetwarzania danych, w tym zakazu przetwarzania, nakazanie sprostowania lub usunięcia danych.
To tylko jedne z wielu możliwych uprawnień naprawczych.

Jak pokazuje praktyka, kara finansowa nałożona przez PUODO na przedsiębiorcę wcale nie musi być najbardziej odczuwalna ekonomicznie spośród innych sankcji wynikających z danej decyzji. Tytułem przykładu, wskazać należy, że pierwszą karą finansową Urząd nałożył na podmiot, który – jak uznał PUODO – nie wypełnił obowiązku informacyjnego wobec osób, których dane przetwarzał (dane pobierał z publicznych rejestrów, a następnie udostępniał je na swojej stronie internetowej w celu prowadzenia działalności gospodarczej). Na przedsiębiorcę nałożono karę w wysokości ok. miliona złotych. Jednak bardziej dotkliwe okazało się zobowiązanie go do wykonania wstecz obowiązku informacyjnego wobec tych sześciu milionów osób, które takiej informacji nie otrzymały. Konieczność dokonania takich zawiadomień w drodze tradycyjnej korespondencji pocztowej (z uwagi na nieposiadanie adresów mailowych tych osób) mogło zatem wiązać się z bardzo istotnym kosztem dla przedsiębiorcy, w praktyce dużo wyższym niż sama kara finansowa.

Warto o tym pamiętać. Jak bowiem widać – choćby na powyższym przykładzie – negatywne konsekwencje decyzji Prezesa UODO nie muszą być związane wyłącznie z samymi karami finansowymi, lecz także wykonaniem innych obowiązków z takiej decyzji.

W drugiej z dotychczasowych spraw w Polsce, w której orzeczono karę finansową (sprawa związku sportowego, który ujawnił publicznie bez podstawy prawnej dane osobowe kilkuset sędziów piłkarskich), organ wymierzył taką karę w wysokości ponad pięćdziesięciu pięciu tysięcy złotych. W tym przypadku, podmiot naruszający przepisy o ochronie danych osobowych usunął, co prawda, naruszenia jeszcze w trakcie postępowania przed PUODO, nie uchroniło go to jednakże przez karą. Samo jednak usunięcie naruszeń miało ten skutek, że ww. związek nie musiał dokonywać już po wydaniu decyzji PUODO innych czynności, które wiązałyby się z wydatkami finansowymi.

W tym miejscu warto porównać wymiar kar związanych z naruszeniem przepisów RODO na tle państw członkowskich UE:

1. Niemcy – najwyższa kara 200.000 euro
2. Hiszpania – najwyższa kara 250.000 euro
3. Francja - najwyższa kara 50.000.000 euro
4. Wielka Brytania - najwyższa kara 204.600.000 euro[1]
5. Polska – najwyższa kara 219.538 euro

[1]Kara nie jest ostateczna a jej wysokość może ulec zmianie. Kara dotyczy postępowania Information Commissioner (ICO) – organ nadzorczy Wielkiej Brytanii pko. British Airways

6. Bułgaria – najwyższa kara 27.100 euro

Jak widać, kary nałożone dotychczas w Polsce zbliżone są pod względem wysokości z karami orzekanymi w państwach Europy Zachodniej, a zatem relatywnie wysokie.

ETAP III. Postępowanie sądowo-administracyjne

Wydanie decyzji i odwołanie się od jej postanowień rozpoczyna kolejny etap, a mianowicie – postępowanie sądowo-administracyjne, które toczy się przed sądem. Przedsiębiorca niezgadzający się z decyzją PUODO, ma 30 dni od daty doręczenia mu tej decyzji, na wniesienie skargi do WSA za pośrednictwem PUODO.

Liczne skargi do Urzędu

Wszczęcie postępowania przez organ nadzoru, które może zakończyć się nałożeniem na przedsiębiorcę kary finansowej, najczęściej zaczyna się od złożenia przez osobę, której dane dotyczą, skargi do UODO. Jak wynika z danych opublikowanych przez Prezesa UODO, w okresie od 25 maja 2018 r. do 25 maja 2019 r. do Urzędu wpłynęło 9013 skarg. Dla przykładu, w całym 2017 r. było ich 2950. Nastąpił zatem wzrost o 300 proc.

9013
skarg o naruszenie danych osobowych otrzymał UODO od maja 2018 r. do maja 2019 r.

Z informacji ujawnionych przez UODO wynika, że najczęściej występującymi przyczynami naruszeń są:
- przekazanie danych osobowych do niewłaściwego adresata (głównie drogą elektroniczną),
- utarta (zagubienie, kradzież) nośnika z danymi osobowymi,
- utrata korespondencji przez operatów pocztowych i kurierów.

Jak widać, liczba składanych skarg jest wyższa z roku na rok. Powoduje to konieczność podjęcia przez przedsiębiorców określonych działań, które pozwolą zminimalizować ich zakres odpowiedzialności.

Właściwe działania pozwolą uniknąć kary
Aby zminimalizować ryzyko ukarania, przedsiębiorca powinien podjąć następujące działania:
1. wyznaczyć spośród pracowników osobę odpowiedzialną za kontakt z kontrolerami
Rekomendowane jest, aby tą osobą był wyznaczony w firmie IODO. Jeżeli firma nie wyznaczyła IODO, konieczne jest wskazanie osoby, która będzie posiadała odpowiednie kwalifikacje i kompetencje do tych, które musi posiadać IODO
2. uprzednio przeszkolić pracowników
Przeszkolenie powinno obejmować zakres uprawnień kontrolerów oraz praw i obowiązków administratora danych w trakcie kontroli
3. zgromadzić dokumenty i dowody, o które proszą kontrolujący

W szczególności przedsiębiorca powinien posiadać procedury RODO, a w nich upoważnienia do przetwarzania danych osobowych, a także umowy powierzenia przetwarzania z podmiotami zewnętrznymi, które z nim współpracują

4. zabezpieczyć informacje stanowiące tajemnice przedsiębiorstwa
5. zweryfikować protokoły

Weryfikacją pod kątem prawidłowości ustaleń trzeba objąć zarówno protokoły kontrolne cząstkowe, jak i protokół końcowy

6. złożyć zastrzeżenia do protokołu

Zastrzeżenia należy złożyć w razie stwierdzenia przez firmę naruszeń odnośnie przeprowadzonych przez organ czynności kontrolnych, z którymi przedsiębiorca się nie zgadza/

7. w przypadku problemów – podjąć współpracę z wyspecjalizowanym podmiotem

Zalecane jest przy tym podjęcie współpracy już na etapie kontroli, a nie dopiero w trakcie prowadzonego postępowania przez PUODO

8. stosować się do wytycznych kontrolerów i PUODO.

Prawidłowa i rzetelna realizacja ww. czynności powinna skutkować spokojnym i sprawnym przebiegiem czynności kontrolnych, co leży w interesie samego przedsiębiorcy.

Autorzy:
Łukasz Zboralski, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.
Michał Dutkiewicz, prawnik, Kancelaria Prawna Piszcz i Wspólnicy sp.k.