Dziennik Gazeta Prawna Tygodnik
01.02.19 nr: 5 str. 9 nakład: 47000 egz.

Już wiadomo, kogo skontroluje UODO. Teraz trzeba się przygotować

Urszula Wróblewska
urszula.wroblewska@infor.pl

To nie przelewki. Nawet do 20 mln euro lub 4 proc. wartości rocznego światowego obrotu przedsiębiorstwa – tyle może wynieść kara dla firmy, która naruszy ogólne rozporządzenie o ochronie danych osobowych 2016/679, czyli RODO. Czy Urząd Ochrony Danych Osobowych, który w ubiegłym tygodniu opublikował plan kontroli sektorowych, sięgnie po tak drastyczne sankcje? Niewykluczone, ich dotkliwość ma bowiem odstraszać podmioty nieprawidłowo przygotowane do przetwarzania danych. I nie jest ważne, czy firma jest polska czy zagraniczna, wysokość kar dla wszystkich jednakowa. Spać spokojnie nie mogą także instytucje publiczne (jednostki sektora finansów publicznych), które za niefrasobliwość związaną z przetwarzaniem danych osobowych mogą ponieść karę do 100 tys. zł.

Do zapowiedzianych przez UODO kontroli trzeba się na pewno przygotować. Przede wszystkim warto zrobić analizę, czy o wszystko należycie zadbaliśmy – pamiętajmy o tym, że zgodność z RODO oznaczała dla przedsiębiorców konieczność wprowadzenia zmian zarówno w obszarze prawnym, jak i technologicznym czy bezpieczeństwa. Warto też wiedzieć, jak będzie przebiegała kontrola RODO, a także poznać swoje obowiązki i prawa. Tym bardziej że przepisy są nowe i w wielu przypadkach trudno dziś jednoznacznie stwierdzić, jak poszczególne kwestie będą interpretowane oraz jakie działania podjąć. Aby im zadośćuczynić. Same przepisy są bowiem dość jednoznaczne (oczywiście na ile to możliwe na poziomie przepisu). Trudno wymagać od ustawodawcy większej szczegółowości. Wątpliwości interpretacyjne więc zawsze pozostają. Dlatego dziś, wychodząc naprzeciw oczekiwaniom naszych czytelników, przedstawiamy praktyczny poradnik dotyczący kontroli UODO, którego pracownicy wkrótce zapukają do drzwi wielu firm. Nasi eksperci nie tylko opisują krok po kroku procedurę i podpowiadają, w jaki sposób się zachować w konkretnych sytuacjach, ale również odpowiadają na najczęściej zadawane pytania podmiotów zbierających, przetwarzających i przechowujących dane.

DR DOMINIKA DÖRRE-KOLASA
radca prawny, partner w kancelarii Raczkowski Paruch w Krakowie

ROBERT STĘPIEŃ
radca prawny w biurze kancelarii Raczkowski Paruch w Krakowie

AGNIESZKA NICIŃSKA
prawnik w biurze kancelarii Raczkowski Paruch w Krakowie

Wyznaczono kierunki działania

Banki, firmy ubezpieczeniowe, telemarketing, brokerzy danych, a nawet spółdzielnie mieszkaniowe. Do tego sektor publiczny w zakresie miejskiego monitoringu wizyjnego czy udostępniania informacji w BIP – to m.in. znalazło się w rocznym planie kontroli Urzędu Ochrony Danych Osobowych na 2019 r.

Kontrole przestrzegania przepisów o ochronie danych osobowych mogą być prowadzone bez uprzedzenia. Administratorzy danych osobowych powinni więc niezwłocznie zweryfikować, czy procesy przetwarzania są przeprowadzane zgodnie z przepisami dotyczącymi ochrony danych osobowych oraz dostosować do nich praktykę. Na co konkretnie powinni zwrócić uwagę i jakie działania podjąć, biorąc pod uwagę przedmiot zapowiadanych kontroli? O tym za chwilę.

Zacznijmy najpierw od tego, kto jest na cenzurowanym.

Zakresem planowanych kontroli zostały objęte w szczególności następujące podmioty i zagadnienia:

1) wszyscy pracodawcy – przetwarzanie danych osobowych rejestrowanych za pomocą monitoringu wizyjnego oraz przetwarzanie danych w związku z rekrutacją;
2) podmioty z sektora bankowego i ubezpieczeniowego – profilowanie danych;
3) telemarketing – stosowany przez podmioty z sektora prywatnego;
4) brokerzy danych – podstawy prawne przetwarzania danych osobowych (szczegółowa lista – patrz infografika, s. C11).

Nie oznacza to jednak, że wszyscy inni mogą spać spokojnie. Pamiętajmy bowiem, że poza kontrolami prowadzonymi zgodnie z zatwierdzonym przez prezesa Urzędu Ochrony Danych Osobowych planem ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm., dalej: u.o.d.o.) wyróżnia jeszcze kontrole prowadzone:

- na podstawie informacji uzyskanych przez prezesa UODO,
- kontrolę prowadzoną w ramach monitorowania przestrzegania stosowania RODO.

Kto zapuka do firm lub instytucji

Do wszczęcia kontroli uprawnieni są wyłącznie:

- pracownicy Urzędu Ochrony Danych Osobowych;
- członkowie lub pracownicy innego organu nadzorczego państwa członkowskiego Unii Europejskiej – w przypadku prowadzenia wspólnych operacji organów nadzorczych.

Uwaga! Pracownicy innych organów niż wymienione powyżej nie mogą wszcząć kontroli przestrzegania przepisów o ochronie danych osobowych. Mogą jednak przy okazji prowadzenia swoich czynności weryfikować niektóre aspekty. Ot, jak chociażby Państwowa Inspekcja Pracy, która może sprawdzać stosowanie monitoringu. Przestrzeganie przepisów dotyczących ochrony danych osobowych będzie także jednym z elementów kontroli przeprowadzanej przez Najwyższą Izbę Kontroli.

Czasami w czynnościach mogą uczestniczyć dodatkowe, posiadające specjalistyczną wiedzę osoby. Działają one wówczas na podstawie upoważnienia nadanego przez prezesa urzędu, przy czym powinny brać udział jedynie w wyznaczonych czynnościach.

Co może kontrolowany

Jego udział w czynnościach kontrolnych jest obowiązkowy, a ponadto musi też (na piśmie) wskazać osobę upoważnioną do reprezentowania go w trakcie kontroli. W związku z powyższym kontrolowany lub upoważniona przez niego osoba mają prawo w każdej sytuacji domagać się dopuszczenia do udziału w czynnościach. Podejmując decyzję o wyznaczeniu określonej osoby jako upoważnionej do reprezentowania go w trakcie kontroli, należy wziąć pod uwagę przede wszystkim jej wiedzę i doświadczenie w zakresie ochrony danych osobowych. W szczególności taka osoba powinna być zaznajomiona z zakresem działalności kontrolowanego oraz posiadać określone predyspozycje osobowościowe, tak aby czuwać nad przebiegiem czynności i dbać o ochronę praw kontrolowanego.

Uważamy, że samo wskazanie osoby upoważnionej do reprezentowania kontrolowanego może być niewystarczające. Rekomendujemy zapewnienie takiej osobie odpowiedniego zaplecza organizacyjno-technicznego – w celu bieżącego wsparcia jej w trakcie czynności kontrolnych (będzie to szczególnie istotne w przypadku konieczności złożenia w terminie siedmiu dni zastrzeżeń do protokołu kontroli).

Uwaga! Nieobecność kontrolowanego bądź osoby przez niego upoważnionej nie wstrzymuje wszczęcia kontroli. W takiej sytuacji upoważnienie do jej przeprowadzenia może zostać okazane:

- osobie czynnej w lokalu przedsiębiorstwa, wykonującej czynności bezpośrednio związane z prowadzeniem działalności przedsiębiorstwa, o ile taki lokal jest przeznaczony do obsługiwania publiczności, bądź
- przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym w rozumieniu kodeksu karnego.

Tak to będzie przebiegało

KROK 1. WSZCZĘCIE KONTROLI

Kontrola przestrzegania przepisów o ochronie danych osobowych rozpoczyna się w momencie okazania imiennego upo-

Dziennik Gazeta Prawna Tygodnik
01.02.19 nr: 5 str. 9 nakład: 47000 egz.

Stanowisko Urzędu Ochrony Danych Osobowych z 31.01.2019 r.

Prezes Urzędu Ochrony Danych Osobowych, wybierając sektory do kontroli, kierowała się m.in. licznymi sygnałami (w tym skargami, pytaniami i zgłoszeniami naruszeń ochrony danych osobowych) wskazującymi na zagrożenia naruszenia przepisów o ochronie danych osobowych. Decyzja o sprawdzeniu jakiegoś sektora bywa też podejmowana pod wpływem zmian prawa w danym obszarze. Impulsem do podjęcia tego typu działań bywają także doniesienia medialne. Ponadto kontrole UODO są podejmowane w związku z potrzebą zweryfikowania, jak w praktyce realizowane są wskazówki i zalecenia urzędu zawarte w naszych poradnikach, stanowiskach i wytycznych. Przykładem jest np. monitoring wizyjny, którego kontrole rozpoczęły się w 2018 r. i będą kontynuowane także w tym roku. Kwestia przetwarzania danych osobowych przez pracodawców, także w zakresie prowadzenia rekrutacji, to kolejny taki przykład.
W przeszłości generalny inspektor ochrony danych osobowych (GIODO, dziś UODO) dostrzegał w wielu branżach problemy związane z przetwarzaniem danych. Przykładowo w sektorze prywatnym wiele wątpliwości budziła działalność podmiotów zajmujących się marketingiem. Nie uwzględniały sprzeciwu osób, których dane były przetwarzane, nie informowały o źródle pozyskania danych osobowych czy przetwarzały dane bez zgody.
Dużo wątpliwości dotyczyło sektora finansowego w tym banków, które np. przekazywały do Biura Informacji Kredytowej dane klientów, gdy nie było do tego podstawy prawnej. W przypadku firm telekomunikacyjnych dochodziło np. do pozyskiwania nadmiarowych danych przy zawieraniu umów.
Również sklepy internetowe często pozyskiwały nadmiarowe dane o swoich klientach, podczas logowania do systemów sprzedażowych. W przypadku pozyskiwania danych nowych klientów nie informowały o tym, że weszły w posiadania ich danych albo nieprawidłowo realizowały ten obowiązek.
W przypadku sektora publicznego problemami, które często miały miejsce, były: pozyskiwanie nadmiarowych danych przez instytucje publicznych (żądanie nieadekwatnych danych), brak odpowiednich zabezpieczeń w systemach informatycznych. Często dochodziło do publikowania zbyt szerokiego zakresu danych w Biuletynie Informacji Publicznej lub na stronach internetowych poszczególnych instytucji.
Chcemy podkreślić, że fakt wydania przez Ministerstwo Cyfryzacji objaśnień prawnych dotyczących gromadzenia danych osobowych kandydatów do pracy po zakończeniu rekrutacji nie miał wpływu na wybór przez prezesa UODO takiego obszaru do kontroli.

Not. **J.S**

ważnienia do jej przeprowadzenia wraz z legitymacją służbową (jeżeli jest przeprowadzana przez pracownika urzędu) bądź dokumentem tożsamości (w przypadku prowadzenia jej przez członka lub pracownika innego organu nadzorczego państwa członkowskiego). Przy czym upoważnienie do przeprowadzania kontroli powinno zawierać:

- wskazanie podstawy prawnej przeprowadzenia kontroli;
- oznaczenie organu;
- imię i nazwisko, stanowisko służbowe kontrolującego oraz numer legitymacji służbowej, a w przypadku prowadzenia wspólnych operacji organów nadzorczych – imię, nazwisko oraz numer dokumentu potwierdzającego tożsamość członka lub pracownika innego organu nadzorczego państwa członkowskiego Unii Europejskiej;
- określenie zakresu przedmiotowego kontroli;
- oznaczenie kontrolowanego;
- wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności;
- podpis prezesa UODO;
- pouczenie kontrolowanego o jego prawach i obowiązkach;
- datę i miejsce jego wystawienia.

W przypadku stwierdzenia braków w upoważnieniu rekomendujemy kontakt z urzędem w celu wyjaśnienia wątpliwości, w szczególności z uwagi na pojawiające się w opinii publicznej informacje o fałszywych kontrolujących.

KROK 2. PRZEBIEG KONTROLI, CZYLI CO WOLNO KONTROLUJĄCEMU

Ustawa o ochronie danych osobowych przyznaje kontrolującym wiele uprawnień w celu skutecznego przeprowadzenia czynności. Najważniejsze z nich to:

- **prawo wstępu na grunt oraz do budynków, lokali i innych pomieszczeń kontrolowanego**

Miejsca, w których prowadzone będą czynności, powinny być ściśle związane z prowadzoną przez kontrolowanego działalnością. Co więcej, miejsca te powinny być powiązane z zakresem kontroli określonym w upoważnieniu do jej przeprowadzenia. Prawo takie przysługuje kontrolującemu od godz. 6.00 do godz. 22.00. Wydaje się jednak, że przeprowadzanie czynności na terenie i w pomieszczeniach kontrolowanego powinno odbywać się w godzinach i dniach jego pracy, a wyjątki od tej zasady powinny być stosowane jedynie w szczególnych okolicznościach. Ponadto w sytuacji, gdy na jednym obszarze działalność prowadzi kilku administratorów, pozostali nie powinni być objęci kontrolą.

- **prawo wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli**

To niezwykle istotne uprawnienie. Nie oznacza ono jednak, że prowadzący czynności z upoważnienia prezesa UODO mogą żądać wglądu do wszelkich informacji i dokumentów będących w posiadaniu kontrolowanego. Prawo to jest ograniczone jedynie do dokumentów związanych z przetwarzaniem danych osobowych, które mają bezpośredni związek z zakresem przedmiotowym kontroli – wynikającym z upoważnienia do jej przeprowadzenia.

Ustawa o ochronie danych osobowych co do zasady przyznaje prezesowi UODO prawo dostępu do informacji objętych tajemnicą prawnie chronioną. Ale uprawnienie to zostaje wyłączone, gdy przepisy szczególne tak stanowią. Przykładem tajemnicy prawnie chronionej będzie tajemnica adwokacka, radcy prawnego czy bankowa. Przy czym projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, który wskazuje, że obowiązek zachowania tajemnicy zawodowej adwokata bądź radcy prawnego nie ustaje nawet w przypadku, gdy z żądaniem ujawnienia informacji uzyskanych przez nich w związku ze świadczeniem pomocy prawnej występuje prezes Urzędu Ochrony Danych Osobowych, nadal procedowany jest w Sejmie.

Ustawodawca przyznał też kontrolowanemu prawo zastrzeżenia informacji, dokumentów lub ich części zawierających tajemnicę przedsiębiorstwa. Chodzi o informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął – przy zachowaniu należytej staranności – działania w celu utrzymania ich w poufności.

Uwaga! Mimo zgłoszenia zastrzeżenia informacji kontrolujący i tak powinien przedstawić prezesowi UODO dwie wersje dokumentu: jedną oryginalną, zawierającą informacje stanowiące tajemnicę przedsiębiorstwa, oraz drugą – niezawierającą informacji objętych zastrzeżeniem. W przypadku niedostarczenia wersji dokumentu niezawierającej informacji objętych zastrzeżeniem, zastrzeżenie uważa się za nieskuteczne.

Przy czym zastrzeżenie zgłoszone przez kontrolowanego nie ma charakteru bezwzględnego. Prezes UODO może uchylić je w drodze decyzji, jeżeli uzna, że informacje, dokumenty lub ich części nie spełniają przesłanek do objęcia ich tajemnicą przedsiębiorstwa. Postępowanie przed prezesem urzędu jest postępowaniem jednoinstancyjnym. W konsekwencji wydane przez niego decyzje urzędu są ostateczne i wykonalne z mocy samego prawa z chwilą doręczenia decyzji stronie. Decyzja administracyjna wydana przez prezesa UODO, uchylająca zastrzeżenie, może być następnie przedmiotem skargi do sądu administracyjnego.

Ponadto warto pamiętać, że prezes urzędu może żądać przetłumaczenia na język polski dokumentacji sporządzonej w języku obcym. Obowiązek ten będzie szczególnie uciążliwy dla przedsiębiorstw wchodzących w skład grup kapitałowych, które z reguły posiadają dokumentację w języku angielskim. Tym bardziej że tłumaczenia dokumentów kontrolowany dokonuje na własny koszt. W związku z powyższym rekomendujemy, aby najważniejsze dokumenty z zakresu danych osobowych już teraz przetłumaczyć na język polski.

- **prawo do przeprowadzania oględzin**

Kontrolujący są uprawnieni do przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych. W praktyce oględzinom podlegać mogą archiwa i inne miejsca przechowywania dokumentów zawierających dane osobowe, miejsca z podglądem do monitoringu czy systemy informatyczne. W tym ostatnim przypadku kontrolujący będą mieli możliwość zapoznania się ze sposobem funkcjonowania danego systemu oraz ze stosowanymi zabezpieczeniami.

- **prawo żądania pisemnych lub ustnych wyjaśnień oraz przesłuchania w charakterze świadka**

Kontrolujący zgodnie z ustawą mają prawo żądać pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka każdego, czyje zeznania lub wyjaśnienia mogą okazać się niezbędne do ustalenia stanu faktycznego.

Oznacza to, że kontrolujący mają np. uprawnienia do żądania wyjaśnień nawet od klientów kontrolowanego.

Odmiennie uregulowano natomiast kwestię zeznań składanych w charakterze świadka przez osobę będącą pracownikiem kontrolowanego. Przy czym za pracownika uznaje się nie tylko osoby zatrudnione na podstawie umowy o pracę, ale również zatrudnione na podstawie umów cywilnoprawnych.

Warto też pamiętać, że pracownik kontrolowanego składający zeznania w charakterze świadka ma prawo odmówić ich złożenia, jeżeli jest małżonkiem, wstępnym, zstępnym, rodzeństwem kontrolowanego oraz jego powinowatym pierwszego stopnia lub pozostaje z nim w stosunku przysposobienia, opieki lub kurateli. Uprawnienie to może być więc stosowane tylko w sytuacji, gdy kontrolowanym będzie osoba fizyczna. Z kolei wszyscy pracownicy mają możliwość odmowy odpowiedzi na konkretne pytania w przypadku, gdy odpowiedź mogłaby narazić ich lub ich bliskich na odpowiedzialność karną, hańbę lub bezpośrednią szkodę majątkową albo spowodować naruszenie obowiązku zachowania prawnie chronionej tajemnicy zawodowej.

Uwaga! Za składanie zeznań i wyjaśnień zgodnych z prawdą w stosunku do pracownika nie mogą być stosowane żadne negatywne konsekwencje. W szczególności nie jest dopuszczalne rozwiązanie umowy o pracę bądź stosowanie kar porządkowych.

- **prawo do zlecania sporządzania ekspertyz i opinii**

Jeżeli informacje, z którymi zapoznają się kontrolujący, będą wymagały wiadomości specjalistycznych z uwagi na złożoność procesów przetwarzania danych, mogą oni skorzystać z pomocy podmiotów przygotowujących ekspertyzy i opinie w niezbędnym zakresie.

- **prawo żądania kopii lub wydruków**

Na żądanie kontrolujących kontrolowany musi sporządzić kopię dokumentów przechowywanych w formie papierowej. W sytuacji gdy dokumenty są prowadzone w formie elektronicznej, kontrolowany będzie natomiast zobowiązany do ich wydrukowania bądź przeniesienia na nośnik informacji i przekazania kontrolującym. Koszt wykonania kopii i wydruków obciąża kontrolowanego.

- **prawo żądania potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków**

Na kontrolowanym ciąży też obowiązek potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków. A gdy odmówi lub nie dokona takiego potwierdzenia, kontrolujący będzie musiał uczynić o tym wzmiankę w protokole kontroli. Ustawa w takiej sytuacji w stosunku do kontrolowanego nie przewiduje żadnych sankcji.

- **prawo utrwalenia przebiegu kontroli**

Kontrolujący w uzasadnionych przypadkach jest uprawniony do utrwalenia przebiegu kontroli lub poszczególnych jej czynności za pomocą urządzeń rejestrujących dźwięk lub obraz. Takie sformułowanie przepisu sprawia jednak, że w praktyce od subiektywnej oceny kontrolującego zależy, czy w danym przypadku skorzysta z powyższej możliwości. Uzasadnione okoliczności mogą zachodzić w szczególności, gdy procesy przetwarzania danych osobowych są skomplikowane i może dojść do pominięcia istotnych informacji w protokole kontroli lub gdy składane przez pracowników zeznania pozostają ze sobą w sprzeczności.

Uwaga! Warunkiem utrwalenia przebiegu kontroli jest uprzednie poinformowanie o tym kontrolowanego. Ponadto urządzenia, na których zapisano przebieg kontroli lub poszczególnych czynności, będą stanowiły załącznik do protokołu kontroli. Dzię-

ki temu kontrolowany w razie wątpliwości może wykazać, że ustalenia zawarte w protokole nie odpowiadają stanowi faktycznemu bądź przebiegowi kontroli.

KROK 3. ZAKOŃCZENIE KONTROLI

Kontrolujący ustala stan faktyczny na podstawie dowodów zebranych w postępowaniu kontrolnym, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg czynności jest utrwalony w protokole kontroli (może być sporządzony zarówno w formie pisemnej, jak i elektronicznej), który powinien zawierać:

- wskazanie nazwy albo imienia i nazwiska oraz adresu kontrolowanego;
- imię i nazwisko osoby reprezentującej kontrolowanego oraz nazwę organu reprezentującego kontrolowanego;
- imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer imiennego upoważnienia kontrolującego, a w przypadku członka lub pracownika organu nadzorczego państwa członkowskiego Unii Europejskiej uczestniczącego we wspólnych operacjach organów nadzorczych imię i nazwisko, numer dokumentu potwierdzającego tożsamość oraz numer imiennego upoważnienia;
- datę rozpoczęcia i zakończenia czynności kontrolnych;
- określenie zakresu przedmiotowego kontroli;
- opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
- wyszczególnienie załączników;
- omówienie dokonanych w protokole kontroli poprawek, skreśleń i uzupełnień;
- pouczenie kontrolowanego o prawie zgłaszania zastrzeżeń do protokołu kontroli oraz o prawie odmowy podpisania protokołu kontroli;
- datę i miejsce podpisania protokołu kontroli przez kontrolującego i kontrolowanego.

Jednym z obligatoryjnych elementów protokołu jest wyszczególnienie załączników. W związku z powyższym wydaje się, że do protokołu nie będą załączone kopie i wydruki wszystkich dokumentów, których żądali kontrolujący.

Kontrolowany w terminie siedmiu dni kalendarzowych od dnia otrzymania protokołu musi go podpisać bądź złożyć pisemne zastrzeżenia co do jego treści. Złożenie zastrzeżeń umożliwia ustosunkowanie się do stwierdzeń i uwag zawartych w protokole. Ponadto zastrzeżenia mogą dotyczyć zakresu przeprowadzanej kontroli bądź braków w ustaleniu stanu faktycznego. Protokół bądź złożone zastrzeżenia powinny zostać w powyższym terminie doręczone kontrolującemu. W przypadku skutecznego złożenia pisemnych 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 w formie aneksu.

Uwaga! Ustawodawca nie sprecyzował, w jaki sposób powinno nastąpić doręczenie protokołu bądź zastrzeżeń do jego treści. Podpisany protokół w formie pisemnej powinien na pewno zostać doręczony na adres kontrolującego. W przypadku otrzymania protokołu w formie elektronicznej wydaje się, że istnieje możliwość posługiwania się podpisem elektronicznym. Aby uniknąć wątpliwości, rekomendujemy uzgodnienie z kontrolującymi jeszcze na etapie kontroli sposobu doręczenia protokołu bądź zastrzeżeń.

Jeżeli kontrolowany odmówi podpisania protokołu, kontrolujący uczyni o tym wzmiankę w protokole, która musi zawierać datę jej dokonania. Równoznaczny z odmową podpisania protokołu jest brak doręczenia podpisanego protokołu kontroli oraz brak zgłoszenia zastrzeżeń do jego treści. W takiej sytuacji kotrolujący uczyni w protokole odpowiednią wzmiankę o braku doręczenia podpisanego protokołu i niezgłoszeniu zastrzeżeń wraz z datą, która będzie jednocześnie terminem zakończenia kontroli.

Dziennik Gazeta Prawna Tygodnik
01.02.19 nr: 5 str. 9 nakład: 47000 egz.

O TO PYTAJĄ ADMINISTRATORZY

Przedmiotem kontroli będzie w szczególności monitoring wizyjny. Co w przypadku gdy pracodawca nie uregulował tego w regulaminie pracy? Rozumiem, że powinien niezwłocznie to zrobić.

Niekoniecznie. Zanim to zrobi, powinien w pierwszej kolejności ustalić, na jakiej podstawie monitoring wizyjny jest stosowany. Czy wynika to z obowiązku prawnego ciążącego na pracodawcy, czy jest jedynie wynikiem jego decyzji podjętej w jednym z celów wskazanych w kodeksie pracy, a więc w szczególności w celu zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Jeżeli stosowanie monitoringu wynika z obowiązku prawnego ustalonego na podstawie odrębnych przepisów, nie stosuje się wymogów wynikających z kodeksu pracy, w tym obowiązku wprowadzenia regulacji dotyczących monitoringu do regulaminu pracy lub układu zbiorowego. Przykładem takich odrębnych przepisów są przepisy, które nakładają na określone podmioty (np. z sektora bankowego) obowiązki w zakresie ochrony osób i mienia. Jednym ze środków zapewniających ochronę może być monitoring wizyjny. W takim przypadku podstawą jego stosowania jest obowiązek prawny ciążący na pracodawcy, a nie przepisy kodeksu pracy. W związku z tym do stosowania monitoringu nie jest konieczne wprowadzenie zmian do regulaminu pracy lub układu zbiorowego. Jeżeli natomiast podstawą stosowania monitoringu są przepisy kodeksu pracy i prawnie uzasadniony cel administratora danych (określony w tych przepisach), wszystkie przewidziane tam wymogi należy stosować, a więc w szczególności wprowadzić odpowiednie regulacje do regulaminu lub układu.

Czy w świetle celów wymienionych w kodeksie pracy monitoring wizyjny może być wykorzystywany do kontroli tego, czy dany pracownik pojawił się w pracy?

Zgodnie z przepisami kodeksu pracy monitoring wizyjny, o czym już wspominaliśmy, może służyć zapewnieniu bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Jeżeli ustalenie, czy pracownik pojawił się w pracy, jest niezbędne dla realizacji któregoś z wymienionych tutaj celów, to tak – można stosować monitoring wizyjny również w tym zakresie. Przykładowo zweryfikowanie za pomocą monitoringu, czy dany pracownik stawił się w pracy bądź czy nie opuszczał miejsca pracy, może w określonych okolicznościach być niezbędne do realizacji celu w postaci zapewnienia bezpieczeństwa pracowników lub ochrony mienia i mieścić się w zakresie tego celu. Wymaga to jednak indywidualnego podejścia i zbadania w każdym przypadku, czy rzeczywiście jest to niezbędne.

Kontrole zapowiadane są również co do przetwarzania danych w związku z rekrutacją. Jak długo pracodawca może przechowywać i przetwarzać dane osobowe znajdujące się w dokumentach rekrutacyjnych osób biorących udział w rekrutacji na konkretne stanowisko?

Prezes Urzędu Ochrony Danych Osobowych stoi na stanowisku, że co do zasady pracodawca powinien trwale usunąć dane osobowe kandydata, z którym nie zdecydował się zawrzeć umowy o pracę, niezwłocznie po zakończeniu procesu rekrutacji. Wyjątki od tej reguły powinny być szczególnie uzasadnione. Co do zasady pracodawca nie będzie więc uprawniony do przetwarzania danych kandydatów do pracy po zakończeniu procesu rekrutacji.

Ministerstwo Cyfryzacji w objaśnieniach z 23 stycznia 2019 r. wskazuje jednak, że po zakończonej rekrutacji pracodawca ma prawo przechowywać dokumentację zawierającą dane osobowe niezatrudnionych osób w celu obrony przed potencjalnymi roszczeniami (np. z tytułu dyskryminacji w procesie rekrutacji). Aby odpowiednio określić okres przechowywania takich danych, pracodawca powinien uprzednio przeprowadzić ocenę ryzyka opierającą się na jego dotychczasowych doświadczeniach w zakresie pojawiających się roszczeń.

Uważamy, że są podstawy do tego, aby przechowywać dokumenty rekrutacyjne po zakończeniu procesu rekrutacji. Takie działanie może być uznane za wykonywanie obowiązku prawnego wynikającego z art. 94 pkt 2b kodeksu pracy, zgodnie z którym pracodawca jest obowiązany przeciwdziałać dyskryminacji w zatrudnieniu. „Przeciwdziałanie" należy w tym przypadku rozumieć nie tylko jako powstrzymywanie się od działań dyskryminujących, ale również jako podejmowanie działań zmierzających do wyeliminowania ryzyka dyskryminacji. W pojęciu tym mieści się w szczególności umożliwienie przeprowadzenia skutecznej kontroli sądowej procesu rekrutacyjnego zakwestionowanego przez kandydata, który nie został zatrudniony. Kandydat, zarzucając pracodawcy dyskryminację, musi wskazać kryterium tej dyskryminacji. W tym celu powinien mieć możliwość uzyskania od pracodawcy odpowiedzi na pytania dotyczące przebiegu postępowania rekrutacyjnego. Z kolei pracodawca, aby mógł rzetelnie odpowiedzieć na takie pytania, musi mieć dostęp do dokumentów rekrutacyjnych. Co więcej, w takim procesie pracodawca musi wykazać obiektywne przyczyny, którymi kierował się, podejmując decyzję odmowną – do tego również niezbędne są wspomniane dokumenty.

Formą przeciwdziałania dyskryminacji może być także kontrola jakości pracy osób odpowiedzialnych za rekrutacje. W tym celu pracodawca powinien mieć możliwość wyrywkowego sprawdzenia przebiegu postępowania rekrutacyjnego, a w szczególności weryfikacji, czy kandydatom zadane zostały analogiczne zestawy pytań, czy właściwie zostały ocenione testy itd. A dokonanie takich czynności sprawdzających nie jest możliwe bez dokumentów aplikacyjnych złożonych przez kandydatów (patrz ramka: Uwaga na objaśnienia prawne Ministerstwa Cyfryzacji).

Wielu pracodawców korzysta z elektronicznych baz kandydatów. W jaki sposób postępować z dokumentacją gromadzoną w takich bazach?

Odpowiedź na to pytanie zależy w szczególności od tego, czy mamy do czynienia z własnymi bazami danych administratora czy z bazami danych zewnętrznych podmiotów (serwisów rekrutacyjnych) zajmujących się publikowaniem ofert zatrudnienia, a następnie gromadzeniem dokumentów rekrutacyjnych osób ubiegających się o zatrudnienie. W pierwszym przypadku pracodawca prowadzący bazę powinien zadbać o jasne i czytelne wyodrębnienie poszczególnych pozycji oraz zapewnienie możliwości bieżącego śledzenia przewidywanego okresu retencji danych dla konkretnych pozycji w bazie. Kontrolujący są uprawnieni do przeprowadzenia oględzin systemów informatycznych, a co za tym idzie do zweryfikowania poprawności przechowywania dokumentacji rekrutacyjnej (w tym okresu jej przechowywania). W przypadku korzystania z elektronicznych baz danych podmiotów zewnętrznych warto odebrać od takiego podmiotu stosowne oświadczenie o zobowiązaniu do usunięcia danych kandydatów po upływie okresu retencji danych. Ponadto pracodawcy powinni mieć zawarte umowy powierzenia przetwarzania danych w przypadku zlecenia rekrutacji na zewnątrz. Bezwzględnie należy uporządkować zawartość dotychczas zgromadzonych baz danych kandydatów – zarówno tych, które znajdują się we własnych zasobach, jak i prowadzonych i przechowywanych na zlecenie.

Niezależnie od powyższego pracodawcy powinni również zwrócić uwagę na sposób postępowania z dokumentacją prowadzoną w formie papierowej. W celu zweryfikowania, czy sposób prowadzenia tej dokumentacji jest zgodny z przepisami dotyczącymi ochrony danych osobowych, zalecane jest przeprowadzenie wewnętrznego audytu – aby uniknąć sytuacji, kiedy w dziale kadr są przechowywane dokumenty rekrutacyjne sprzed kilku lat.

Jakie kwestie mogą być weryfikowane przez kontrolujących w ramach prowadzenia kontroli w obszarze telemarketingu?

Plan kontroli został w tym zakresie sformułowany bardzo ogólnie, a zatem badane aspekty mogą być bardzo różne. Wydaje się jednak, że w czasie kontroli weryfikacji podlegać może legalność dysponowania bazą danych oraz posiadanie odpowiednich zgód marketingowych wynikających z ustawy o świadczeniu usług drogą elektroniczną. Kontrolujący mogą również weryfikować dopełnienie obowiązku informacyjnego czy sposób wykonywania praw przysługujących podmiotom danych (w szczególności prawa do sprzeciwu).

A kiedy będziemy mieli do czynienia z profilowaniem? Na co powinni zwrócić uwagę przedsiębiorcy z sektora bankowego i ubezpieczeniowego?

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. Przykładowo dane mogą być wykorzystywane do analizy lub prognozy efektów pracy osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, lokalizacji lub przemieszczania się.

W przypadku przedsiębiorców z sektora bankowego profilowanie może mieć miejsce przy analizie zdolności kredytowej czy doboru oferty produktów inwestycyjnych. W przypadku firm ubezpieczeniowych profilowanie może dotyczyć oceny analizy stopnia ryzyka ubezpieczeniowego. W jego efekcie może dojść do zautomatyzowanego podjęcia decyzji dotyczącej danej osoby (np. o odmowie przyznania kredytu) albo do przeanalizowania czy dokonania prognozy co do osobistych preferencji takiej osoby. W przypadku sektora ubezpieczeniowego poddanie się profilowaniu może wpłynąć np. na wysokość składki.

Profilowanie co do zasady jest dozwolone, ale może rodzić konieczność spełnienia szczególnych przesłanek – wówczas gdy jest podstawą do podejmowania decyzji – opartej na zautomatyzowanym przetwarzaniu w postaci profilowania – wobec konkretnej osoby. W pozostałych przypadkach profilowania podejmowanego środkami tradycyjnymi podlega ono ogólnym zasadom wynikającym z RODO. Wówczas istnieje jednak ograniczenie w postaci zakazu podejmowania automatycznych decyzji wobec osób, których dane dotyczą, opartych wyłącznie na przetwarzaniu tych danych.

Uwaga na objaśnienia prawne Ministerstwa Cyfryzacji

Resort wydał objaśnienia prawne dotyczące ochrony danych osobowych w procesach rekrutacyjnych. To nowy (wprowadzony przez Konstytucję biznesu), niezwykle cenny instrument gwarantujący tym, którzy się do nich zastosują, uniknięcie kary.

Ale wszystko wskazuje na to, że nie w przypadku kontroli UODO, bo urząd ten nie we wszystkich sprawach zgadza się z MC. I w spornych kwestiach tłumaczenie, że przedsiębiorca zastosował się do wytycznych resortu, nie zagwarantuje 100-proc. ochrony.

Pisaliśmy o tym...

Ministerstwo wyjaśnia, UODO oponuje. A przedsiębiorcy na rozdrożu
Tygodnik Firma i Prawo z 29 stycznia, DGP nr 21


FIRMA i PRAWO
TYGODNIK DLA PRZEDSIĘBIORCÓW
MC wyjaśnia, UODO oponuje. A przedsiębiorcy na rozdrożu
Nazwa apteki też może być niedozwoloną reklamą
Jak dochodzić roszczeń z tytułu regresu