Monitorowanie pracownika zgodne z RODO

W naszym ostatnim artykule pisaliśmy o tym, jak prowadzić monitoring wizyjny w zgodzie z *Ogólnym rozporządzeniem o ochronie danych* oraz przepisami szczególnymi. Teraz przyjrzymy się innym możliwym formom monitorowania aktywności pracowników.

Ramy prawne

Tak jak wykorzystywanie kamer, tak i stosowanie innych technologii do monitorowania pracowników zostało uregulowane przez znowelizowane w maju 2018 r. przepisy *Kodeksu pracy*.

Regulacje art. 22^3 *Kodeksu pracy* określają m.in. granice dopuszczalności stosowania monitorowania, prawa pracowników w tym zakresie oraz obowiązki pracodawcy związane z uruchomieniem oraz utrzymaniem różnych form monitorowania.

Czy natomiast w toku monitorowania będziemy mieli do czynienia z informacjami o charakterze danych osobowych? Zgodnie z definicją art. 4 pkt 1) RODO, dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Pracodawca jest w stanie **łatwo zidentyfikować swojego pracownika**, a zwłaszcza tego, którego aktywność kontroluje. Inaczej taka kontrola nie miałaby przecież większego sensu.

Dodatkowo, w definicji wprost wskazano, że do kategorii danych osobowych należą, w szczególności dane o lokalizacji, a także jeden bądź kilka czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Abstrahując od kwestii lokalizacji, również wyżej wskazane czynniki mogą wynikać z zastosowania innych form monitoringu pracowników. Monitoring lokalizacji auta służbowego nie tylko wskaże nam, gdzie jest pracownik (lokalizacja), ale również pozwoli wywnioskować sposób prowadzenia pojazdu przez pracownika. Natomiast zastosowanie biometrii do kontroli dostępu do serwerowni, będzie wiązało się z przetwarzaniem informacji o czynnikach fizjologicznych.

Tym samym, oprócz przepisów prawa pracy, zastosowanie znajdą również **przepisy RODO**, a w szczególności art. 5 określający zasady przetwarzania danych oraz art. 6 i 9 w zakresie podstaw prawnych przetwarzania tego typu informacji o pracowniku.

Formy monitoringu aktywności pracownika

Kontrolowanie aktywności pracownika w zakładzie pracy, a także poza nim podczas wykonywania przez niego obowiązków służbowych, staje się coraz bardziej popularne. Do tego typu kontroli pracodawcy wykorzystują coraz to nowsze technologie. Część z nich może, w sposób bezpośredni lub pośredni, ingerować w prywatność zatrudnionych osób.

Najczęściej spotykaną formą kontroli jest **monitorowanie służbowej poczty elektronicznej**. Właśnie ten rodzaj nadzoru przewidują wprost przepisy *Kodeksu pracy*. Ustawa nie zamyka jednak katalogu technologii, które mogą być wykorzystywane do monitorowania pracowników. Zwłaszcza, że dotychczasowa praktyka pokazuje, że rzeczywiście jest ich coraz więcej.

Mniej popularne niż przeglądanie wysłanych i odebranych maili, ale również stosowane przez pracodawców, jest **monitorowanie aktywności pracownika w sieci**. Najczęściej przybiera ono jednak formę blokowania konkretnych stron internetowych. Rzadziej, ale również zdarza się, że pracodawca analizuje całą historię aktywności w tym zakresie.

Wśród pracodawców udostępniających swoim pracownikom samochody służbowe rośnie trend umieszczania w pojazdach **lokalizatorów GPS**. Natomiast tam, gdzie podstawowym narzędziem pracy jest telefon służbowy, zdarza się **kontrola bilingów rozmów telefonicznych**.

Oczywiście nie są to jedyne formy kontroli jakie może zastosować pracodawca. Granice w tym zakresie wyznacza nie tylko jego fantazja czy dostępna technologia, ale przede wszystkim **sfera prywatności pracownika i odpowiednie przepisy**.

Ograniczenie celów

Pracodawca **nie ma prawa** do naruszania prywatności pracownika w miejscu pracy (na przykład poprzez śledzenie korespondencji e-mail czy sprawdzanie lokalizacji samochodu kierowanego przez pracownika) **bez poważnego powodu związanego z charakterem jego pracy**.

Prowadzony nadzór nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Kontrola może być wprowadzona **jedynie w celach** wskazanych w art. 22^3 *Kodeksu pracy*, tj. **jeżeli jest to niezbędne do**:

- **zapewnienia organizacji pracy** umożliwiającej pełne wykorzystywanie czasu pracy, lub
- **właściwego użytkowania** udostępnionych pracownikowi **narzędzi pracy**.

Oznacza to, że zasadniczym celem, dla którego pracodawca wprowadza jakąkolwiek formę monitoringu aktywności pracownika powinna być chęć zapewnienia, że pracownik nie jest zbytnio obciążony pracą oraz wykorzystuje powierzone mu narzędzia do celów zawodowych.

Podstawy prawne stosowania kontroli

Tak jak w przypadku instalacji kamer, tak i w przypadku wprowadzania innych form monitoringu aktywności pracownika, przesłanki legalizujące takie działanie będą różnić się w zależności od tego z jakim podmiotem mamy do czynienia. Inaczej bowiem będą wyglądały podstawy prawne zbierania danych przez podmioty publiczne, a inaczej przez podmioty prywatne.

Dla **podmiotów prywatnych** przesłankę do przetwarzania danych w ramach kontroli pracownika stanowi art. 6 ust. 1 lit. f) *Ogólnego rozporządzenia o ochronie danych*, czyli tzw. **prawnie uzasadniony interes administratora**. W tym przypadku, uzasadnionym interesem pracodawcy będzie przede wszystkim zapewnienie właściwej organizacji pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

Zgodnie z motywem 47 RODO, prawnie uzasadniony interes administratora nie ma zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Dlatego też w ich przypadku podstawę monitoringu aktywności pracownika stanowić będą:

- art. 6 ust. 1 lit. c) *Ogólnego rozporządzenia o ochronie danych* – przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego** ciążącego na administratorze (tylko kiedy przepis prawa jasno wskazuje na obowiązek), lub

- art. 6 ust. 1 lit. e) *Ogólnego rozporządzenia o ochronie danych* – przetwarzanie jest niezbędne do wykonania zadania realizowanego w **interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi** (jeżeli brak obowiązku (tj. uprawnienie) lub w ogóle brak przepisu prawa).

W żadnym wypadku **podstawy** dla przetwarzania danych osobowych pracowników w związku z wprowadzonym monitoringiem aktywności **nie powinien stanowić** art. 6 ust. 1 lit. a) *Ogólnego rozporządzenia o ochronie danych* tj. **zgoda**. Już Generalny Inspektor Ochrony Danych Osobowych (poprzednik Prezesa Urzędu Ochrony Danych Osobowych) zwracał w swoich decyzjach uwagę na to, że tak wyrażona zgoda **może nie posiadać cechy dobrowolności**, która jest warunkiem, aby zgoda była uznana za ważną (m.in. decyzja z dnia 22 lutego 2008 r. sygn. DIS/DEC- 134/4605/08, decyzja z dnia 9 grudnia 2009 r. sygn. DIS/DEC- 1261/46988/09). Także Naczelny Sąd Administracyjny przyjął jednoznaczne stanowisko, iż wyrażona na prośbę pracodawcy zgoda pracownika na pobranie i przetwarzanie jego danych osobowych**, narusza prawa pracownika i swobodę wyrażenia przez niego woli** (wyrok z dnia 1 grudnia 2009 r. sygn. akt I OSK 249/09). NSA podkreślił w szczególności **brak równowagi w relacji pracodawca pracownik**.

Tym samym, pracodawca decydując się na taką przesłankę przetwarzania w zakresie kontrolowania aktywności pracownika naraża się na niebezpieczeństwo, że pozyskana zgoda zostanie uznana za nieważną. Oczywiście, jeżeli faktycznie zapewni on, że zgoda pracownika będzie w pełni dobrowolna oraz będzie spełniała inne warunki art. 7 RODO (w tym pracownik będzie mógł ją wycofać), taka podstawa prawna może być wykorzystywana. Biorąc jednak pod uwagę cele kontroli trudno wyobrazić sobie sytuacje, gdzie pracownik faktyczne, bez żadnych negatywnych konsekwencji będzie mógł zgody nie wyrazić bądź udzieloną zgodę wycofać. Dlatego też, nie rekomendujemy korzystania z tej przesłanki przetwarzania w omawianym zakresie.

Monitoring a prywatność pracownika

Wprowadzenie jakiejkolwiek z form monitorowania pracownika może mieć zasadniczy wpływ na jego prywatność oraz inne dobra osobiste. Przed ich wprowadzeniem pracodawca powinien dokonać szczegółowej analizy, czy rzeczywiście dla osiągniecia założonego celu taki monitoring jest w ogóle konieczny. Jeżeli cel może zostać osiągnięty na kilka różnych sposobów, to należy wybrać ten, który **jak najmniej ingeruje w prywatność pracownika** (m.in. zgodnie z zasadą *privacy by default*).

Przykładowo, decydując się na wprowadzenie monitoringu poczty elektronicznej, pracodawca powinien pamiętać, że **nie może kontrolować prywatnej korespondencji swoich pracowników**. Takie zachowanie naruszałoby konstytucyjne prawo do prywatności. Ponadto, monitoring poczty elektronicznej **nie może naruszać tajemnicy korespondencji** oraz innych dóbr osobistych pracownika.

Na uwagę zasługuje przy tym wyrok Europejskiego Trybunału Praw Człowieka z dnia 3 kwietnia 2007 r. w sprawie Copland v. Zjednoczone Królestwo. W trakcie zatrudnienia nauczycielki pracodawca monitorował służbowy telefon skarżącej, jej pocztę elektroniczną oraz połączenia internetowe. Kontrola pracodawcy wykazała, że nauczycielka nadużywała służbowego komputera oraz telefonu w celach prywatnych, w konsekwencji czego zwolniono ją z pracy. ETPC w swoim wyroku wskazał, że używanie przez pracowników służbowych telefonów komórkowych czy komputerów będących własnością pracodawcy, **nie oznacza dorozumianej zgody na ich swobodne kontrolowanie**. Pracownik **musi być świadomy możliwości kontrolowania** jego czynności.

Obowiązki pracodawcy w zakresie monitoringu aktywności

Decydując się na wprowadzenie jakiejkolwiek z form monitorowania pracownika, pracodawca musi zrealizować szereg obowiązków wynikających nie tylko z *Kodeksu pracy*, ale również i RODO. Do najważniejszych z nich zaliczymy:

1) **Ustalenie celu, zakresu oraz sposobu zastosowania monitoringu** w układzie zbiorowym pracy lub regulaminie pracy, bądź w obwieszczeniu - jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

Cel, zakres oraz sposób zastosowania monitoringu powinny zostać określone w sposób możliwe jak najbardziej szczegółowy. W szczególności wewnętrzne regulacje powinny wskazywać m.in.:

- **dla monitoringu poczty elektronicznej** – warunki dostępu do służbowej skrzynki mailowej pracownika tj. czy następuje to tylko w przypadku jego dłuższej nieobecności, czy też monitoring prowadzony jest na bieżąco, osoby uprawnione do dokonania przeglądu treści korespondencji, czy do monitoringu wykorzystuje się dedykowane programy (np. stosujące słowa kluczowe) czy też monitoring prowadzony jest „ręcznie" poprzez umożliwienie dostępu z poziomu administratora,

- **dla monitoringu aktywności w sieci** – czy kontrola polega na zablokowaniu stron o określonej treści, czy też monitoring prowadzony jest na bieżąco, a historia aktywności jest zapisywana i analizowana, jeżeli tak, to kto dokonuje analizy,
- **dla monitoringu lokalizacji (GPS)** – czy monitoring obejmuje wyłącznie położenie pojazdu, czy też określa prędkość a także odnotowuje sam fakt włączenia lub wyłączenia silnika, kto może mieć wgląd do tego typu informacji i jak mogą być wykorzystywane, należy ponadto uregulować kwestie związanie z zasadami używania służbowych aut w celach prywatnych tj. czy wówczas pracownik ma możliwość wyłączenia lokalizatora GPS,
- **dla monitoringu bilingów rozmów telefonicznych** – jaki jest zakres monitoringu, czy obejmuje jedynie wykaz połączeń przychodzących i wychodzących, czy również wiadomości tekstowe, wskazanie zasad postępowania przy wykorzystywaniu telefonów służbowych dla celów prywatnych.

2) **Poinformowanie pracowników o planowanym uruchomieniu monitoringu**, najpóźniej na 2 tygodnie przed jego uruchomieniem (poza sytuacjami, kiedy monitoring taki jest już stosowany).

W przypadku nowych pracowników realizacja tego obowiązku powinna nastąpić przed dopuszczeniem ich do pracy. W przypadku pracowników, który zostali już dopuszczeni do pracy, pracodawca powinien poinformować ich o zamiarze monitorowania. Należy przy tym wskazać, że nieprawidłowym będzie prowadzenie monitoringu aktywności obejmującej okres sprzed poinformowania pracownika o zamiarze jego prowadzenia.

3) **Wykonywanie** w stosunku do monitorowanych pracowników **obowiązków informacyjnych** określonych w *Ogólnym rozporządzeniu o ochronie danych* (o obowiązku informacyjnym zgodnym z RODO pisaliśmy w naszym wcześniejszym artykule).

4) **Oznaczenie** monitorowanego obszaru w sposób widoczny i za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

Przykładowo:

- **w przypadku monitoringu poczty elektronicznej** – stosowna informacja mogłaby pojawiać się każdorazowo przy włączaniu przez pracownika komputera lub programu służącego do obsługi poczty elektronicznej,
- **w przypadku monitoringu aktywności w sieci** – stosowna informacja mogłaby pojawiać się każdorazowo przy włączaniu przez pracownika komputera lub przeglądarki internetowej,

- **w przypadku monitoringu lokalizacji (GPS)** – stosowna informacja mogłaby zostać zamieszczona w widocznym miejscu w samochodzie i przybrać formę symbolu obrazkowego informującego o tym, iż trasa pojazdu i jego wykorzystanie będzie monitorowane za pomocą urządzenia lokalizującego,
- **w przypadku monitoringu bilingów rozmów telefonicznych** – stosowna informacja mogłaby przybrać postać drobnej naklejki umieszczonej na tylnej obudowie telefonu.

Czynności związane z przetwarzaniem danych osobowych w związku z wprowadzeniem monitoringu aktywności pracownika powinny zostać ujawnione w rejestrze przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO (jeżeli pracodawca jest zobowiązany do jego prowadzenia). O tym jak prowadzić rejestr czynności przetwarzania pisaliśmy tutaj.

Okres przechowywania danych

Zgodnie z **zasadą ograniczenia przechowywania** (art. 6 ust. 1 lit e) RODO) dane osobowe można przetwarzać przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Uzasadnione cele przetwarzania danych w związku z wprowadzeniem monitoringu aktywności powiązane są z zapewnieniem właściwej organizacji pracy oraz kontrolą właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Zazwyczaj ewentualne nieprawidłowości w korzystaniu z udostępnionych narzędzi pracodawca jest w stanie rozpoznać w przeciągu jednego lub dwóch dni (jeżeli np. korzysta z dedykowanych programów alarmujących o nieprawidłowościach). Rozpoznanie może też nastąpić w późniejszym terminie, jeżeli np. zapisy lokalizacji służbowego samochodu prowadzone są na bieżąco, a ich kontrola i analiza następuje raz w miesiącu. Pracodawca powinien przyjąć takie procedury oraz zasady retencji, aby pozostawać w zgodzie ze wskazaną wyżej zasadą ograniczenia. To, czy dane osobowe są niezbędne dla danego celu, czy nie, powinno być kontrolowane **w możliwie jak najwęższym przedziale czasowym**.

W przypadkach, kiedy zapisy z monitoringu (np. zapis przejazdu pojazdu) stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, przyjęte terminy **mogą ulec przedłużeniu do czasu prawomocnego zakończenia postępowania**.

Ocena skutków dla ochrony danych (DPIA)

Monitoring służbowej poczty elektronicznej, a także inne formy monitoringu pracowników wiążą się przede wszystkim z wykorzystaniem nowych technologii. Tego typu przetwarzanie danych często wiąże się z **wysokim ryzykiem dla praw i wolności osób, których dane dotyczą**.

Pracodawca, który jest zdecydowany na wprowadzenie tej czy innej formy monitoringu aktywności swoich pracowników powinien jeszcze przed jego zastosowaniem przeanalizować, **czy takie działanie będzie podlegało obowiązkom wynikającym z art. 35 RODO**.

Pracodawca jest zobowiązany do przeprowadzenia oceny skutków planowanych operacji przetwarzania, kiedy dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W szczególności zaś, pracodawca powinien zwrócić uwagę na to, czy dany rodzaj operacji przetwarzania został ujawniony w *Wykazie rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony* opracowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO.

Najnowsza wersja wykazu przewiduje, że przeprowadzenia *data protection impact assessment* (DPIA) wymaga się m.in. w przypadku **zakładów pracy**, gdzie wykorzystywane są systemy monitorowania czasu pracy pracowników oraz **przepływu informacji w wykorzystywanych przez nich narzędziach (poczty elektronicznej, Internetu)**. O tym jak zabrać się do przeprowadzenia DPIA pisaliśmy tutaj.

Podsumowanie

Zastosowanie przez pracodawcę jakiejkolwiek formy monitoringu aktywności może wiązać się z ingerencją w sferę prywatną pracownika. Na pracodawcy ciąży obowiązek przeprowadzenia oceny, czy taka ingerencja jest zasadna z uwagi na cele, które chce on osiągnąć. Pomimo tego, że pojęcie życia prywatnego może rozciągać się na działalność zawodową osoby, której dane dotyczą, to warunkiem *sine qua non* stosowania metod nadzoru jest istnienie wyraźnej i precyzyjnej podstawy prawnej tej ingerencji w prywatność.

Autor artykułu:

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

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 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 917 ze zm.)
- Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców (październik 2018)
- Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony