Nowe zalecenia Rady Europy dotyczące przetwarzania danych osobowych pracowników z perspektywy nowych technologii

Katarzyna Żukowska, Rafał Kuchta

nowe technologie [ochrona prywatności] WARDYŃSKI I WSPÓLNICY
czerwiec 2015

Rekomendacja Rady Europy w przedmiocie przetwarzania danych osobowych dla celów zatrudnienia ma odpowiadać na wyzwania związane z postępującą cyfryzacją.

1 kwietnia 2015 r. Komitet Ministrów Rady Europy przyjął rekomendację skierowaną do państw członkowskich Rady Europy dotyczącą zasad, które należy stosować, przetwarzając dane osobowe dla celów zatrudnienia. Poprzednia rekomendacja pochodziła z czasów poprzedzających rozwój internetu i nowych technologii i jako taka nie przystawała do współczesnych realiów. Rada Europy („RE"), mając świadomość zwiększonego wykorzystania nowych technologii oraz środków komunikacji elektronicznej w stosunkach między pracodawcami a pracownikami, podjęła decyzję o jej zmianie, z uwzględnieniem konieczności zapewnienia odpowiedniego poziomu ochrony w zatrudnieniu.

Rekomendacja RE nie ma charakteru wiążącego, niemniej jednak należy liczyć się z tym, że będzie brana pod uwagę przez GIODO oraz sądy przy ocenie zgodności z prawem przetwarzania danych osobowych pracowników, tym bardziej że wskazane w niej zalecenia odpowiadają zasadom przetwarzania danych osobowych określonym przepisami prawa. Zasadne będzie zatem traktowanie rekomendacji jako źródła wskazówek (dobrych praktyk) co do zasad przetwarzania danych osobowych pracowników przy użyciu narzędzi dostarczanych przez nowe technologie.

Poza ogólnymi zasadami przetwarzania danych osobowych w zatrudnieniu rekomendacja odnosi się też do sposobów przetwarzania danych osobowych przy wykorzystaniu konkretnych nowych technologii, w tym internetu i komunikacji elektronicznej w miejscu pracy, systemów i technologii informacyjnych do monitorowania pracowników (m.in. wideonadzór), urządzeń ujawniających miejsce pobytu, wewnętrznych systemów raportowania, a także danych biometrycznych.

Ogólne wytyczne

Zalecenia wskazane w rekomendacji RE zmierzają w dużej mierze do zapewnienia, żeby godność pracowników i kandydatów do pracy, a także ich prawo do prywatności i ochrony danych osobowych nie zostały naruszone, przy jednoczesnym uwzględnieniu potrzeb pracodawców w zakresie pozyskiwania danych osobowych pracowników i kandydatów do pracy, w tym również do monitorowania pracowników.

Aby to osiągnąć, uwzględniono podstawowe zasady przetwarzania danych osobowych, w tym zasady zgodności z prawem, usprawiedliwionego celu, transparentności i proporcjonalności. W odniesieniu do dwóch ostatnich wskazano, że przetwarzanie danych należy ograniczyć jedynie do danych niezbędnych do realizacji celu określonego w poszczególnych przypadkach, zaś dane powinny być zbierane przede wszystkim bezpośrednio od osoby, której dotyczą. Ponadto pracownikowi powinna zostać przekazana informacja dotycząca danych osobowych przetwarzanych przez pracodawcę, w tym m.in. o kategoriach przetwarzanych danych, celu przetwarzania oraz odbiorcach danych.

Szczególne wytyczne dotyczące przetwarzania danych osobowych przy wykorzystaniu nowych technologii

Zgodnie z zaleceniami RE przetwarzanie danych osobowych przy wykorzystaniu nowych technologii wskazanych w rekomendacji wymaga stosowania dodatkowych środków ochronnych. Pracodawca powinien przede wszystkim poinformować pracowników o systemie przed jego wdrożeniem, wskazując, jaki jest cel jego zastosowania, jak długo będą przechowywane dane oraz czy pracownicy mają prawo dostępu do danych i ich poprawiania, a także jak mogą skorzystać z tych praw. Zaleca się również przeprowadzenie konsultacji z przedstawicielami pracowników, a jeśli istnieje ryzyko naruszenia prawa do poszanowania prywatności oraz godności ludzkiej, także uzyskanie zgody tych przedstawicieli.

- ***Internet i komunikacja elektroniczna***

Wiele uwagi poświęcono zagadnieniu wykorzystywania w miejscu pracy internetu lub sieci wewnętrznej oraz urządzeń przeznaczonych do komunikacji elektronicznej. Zasadniczo należy unikać nieuzasadnionej i nieproporcjonalnej ingerencji pracodawcy w prawo pracowników do życia prywatnego. Wśród dopuszczalnych celów ingerencji należy wymienić poprawę efektywności zarządzania, zapewnienie bezpieczeństwa sieci, a także dążenie pracodawcy do zabezpieczenia się przed szkodami wyrządzonymi przez pracowników oraz przed odpowiedzialnością za ich działania.

W razie przetwarzania danych pracowników w związku z korzystaniem przez nich ze stron intra- lub internetowych należy stopniować stosowane środki nadzorcze, zaczynając od rozwiązań łagodniejszych, np. filtrów

blokujących podjęcie określonych działań. W razie stosowania bardziej inwazyjnych rozwiązań, np. monitoringu danych, pierwszeństwo powinien mieć monitoring niezindywidualizowany i losowy na danych anonimowych lub zagregowanych.

Nie może podlegać monitorowaniu korespondencja osobista pracownika prowadzona w miejscu pracy. Natomiast korespondencja zawodowa może być udostępniana, ale tylko gdy jest to konieczne dla celów bezpieczeństwa lub wynika z innych uzasadnionych powodów, np. aby wykryć naruszenie własności intelektualnej pracodawcy czy uzyskać dowody nienależytego wykonywania obowiązków. Pracownik powinien zostać uprzedzony o takiej możliwości.

RE zaleciła także wprowadzenie procedury uzyskiwania dostępu do korespondencji nieobecnego pracownika, tak aby dokonywać tego w jak najmniej inwazyjny sposób, tylko gdy jest to konieczne dla celów zawodowych i po uprzednim poinformowaniu pracownika. Zwrócono również uwagę, że służbowe konta pocztowe powinny być dezaktywowane po odejściu pracowników z pracy. Pracodawca potrzebujący zawartości takiego konta do prowadzenia działalności powinien ją uzyskać jeszcze przed odejściem pracownika, w miarę możliwości w jego obecności.

- ***Informacje dostępne online***

RE zaleca, aby pracodawcy powstrzymali się od żądania od pracowników lub kandydatów do pracy dostępu do informacji, które udostępniają one innym osobom *online*, zwłaszcza za pośrednictwem portali społecznościowych.

- ***Monitorowanie działalności i zachowania pracowników, w tym miejsca pobytu pracownika***

Zdaniem RE nie jest dopuszczalne stosowanie systemów i technologii monitorujących (np. wideonadzór), jeżeli ich bezpośrednim i głównym celem jest monitorowanie działalności i zachowania pracowników. Nie mogą one też służyć do ciągłego sprawdzania jakości i ilości pracy poszczególnych pracowników. Może się zdarzyć, że systemy są wykorzystywane w uzasadnionych celach, takich jak ochrona produkcji, zdrowia, bezpieczeństwa czy zapewnienie skutecznego prowadzenia działalności, lecz pośrednio mają możliwość monitorowania pracowników. Należy je wtedy zaprojektować i ulokować w taki sposób, aby nie naruszać praw podstawowych pracowników. W szczególności monitoring wizyjny nigdy nie powinien obejmować miejsc należących do najbardziej osobistej sfery życia pracowników, takich jak toalety czy szatnie.

Okres przechowywania nagrań powinien być ściśle określony oraz możliwie krótki. Dostęp do nagrań mogą mieć tylko upoważnieni pracownicy w związku z wykonywaniem obowiązków, np. odpowiedzialni za ochronę i bezpieczeństwo zakładu. Jednak pracownik powinien mieć prawo do otrzymania ich kopii w razie wystąpienia sporu lub na potrzeby postępowania sądowego lub administracyjnego.

Analogiczne zasady obowiązują w przypadku technologii pozwalających ustalić położenie pracowników, np. RFID czy GPS. Warto przy tym zauważyć, że mogą one znajdować się nie tylko w urządzeniach cyfrowych, ale też np. w strojach służbowych. Technologie te powinny być wykorzystywane tylko do realizacji uzasadnionych celów pracodawcy, zaś poznanie miejsca przebywania pracownika może stanowić jedynie efekt uboczny. Należy też unikać całodobowego monitorowania pracowników, np. poprzez wyłączenie funkcji lokalizacji poza godzinami pracy.

- ***Dane biometryczne i genetyczne – dane wrażliwe***

W ocenie RE niedopuszczalne jest przetwarzanie danych genetycznych, np. w celu określenia przydatności kandydata do pracy, choćby wyraził on na to zgodę. Wskazuje się bowiem, że wykorzystywanie tego rodzaju danych może prowadzić do dyskryminacji. Od tej zasady można odstąpić jedynie w wyjątkowych okolicznościach, takich jak ochrona zdrowia pracownika lub osoby trzeciej przed ciężkim uszczerbkiem i tylko wtedy, gdy taką możliwość przewiduje prawo krajowe, zapewniając odpowiednie środki ochronne. Jako przykład takich wyjątkowych okoliczności w uzasadnieniu do rekomendacji RE podano monitorowanie efektów biologicznych wywoływanych przez obecne w miejscu pracy substancje toksyczne, przy założeniu, że jest ono wymagane przez prawo albo, w ściśle określonych okolicznościach, w ramach dobrowolnej zgody.

Podobne obostrzenia dotyczą danych biometrycznych obejmujących m.in. dane o liniach papilarnych, obraz siatkówki lub tęczówki oka, głos czy cechy twarzy. Zbieranie i przetwarzanie tych danych jest dopuszczalne, ale tylko wtedy, gdy jest konieczne dla ochrony uzasadnionych interesów pracodawców, pracowników lub osób trzecich i nie istnieją inne, mniej inwazyjne środki pozwalające zrealizować ten interes (proporcjonalność).

W uzasadnieniu rekomendacji wskazano jako przykład takiej sytuacji potrzebę ograniczenia dostępu do pewnych obszarów w instalacjach wojskowych czy elektrowniach jądrowych. Przy przetwarzaniu takich danych należy im zapewnić odpowiednie zabezpieczenia. W uzasadnieniu rekomendacji podkreślono, że dane biometryczne nie powinny być przechowywane w scentralizowanym rejestrze. W miarę możliwości pracownik powinien zachować kontrolę nad danymi, np. dzięki zapisaniu ich na karcie magnetycznej dostępnej wyłącznie dla niego.

Podsumowanie

Powyższe wymogi ograniczają swobodę pracodawcy w wykorzystywaniu nowych technologii dla celów zatrudniania, niemniej jednak wpisują się w ogólną tendencję do zwiększania ochrony prywatności i danych osobowych pracowników. Pozostają one także spójne z podglądami GIODO i sądów powszechnych, które wobec braku jednoznacznego uregulowania powyższych kwestii w przepisach prawa polskiego stanowią wytyczne w obszarze przetwarzania danych osobowych w zatrudnieniu. Organy te w swych rozstrzygnięciach restrykcyjnie oceniają dopuszczalność ingerencji w prywatność pracowników, jak również dopuszczalność przetwarzania pewnych kategorii danych osobowych pracowników (w szczególności danych sensytywnych, do których należą m.in. dane biometryczne). Z tego względu pracodawcy przetwarzający dane osobowe w zatrudnieniu powinni zawsze starannie rozważyć, czy ich działanie jest zgodne z prawem, a także z zasadami proporcjonalności i transparentności, prowadzi do realizacji konkretnego i uzasadnionego celu oraz nie stanowi nadmiernej ingerencji w prawo pracowników do prywatności.