Warszawa, 29.06.2020 r.

**Rozważania na temat roli IOD w sytuacjach spornych**

Na marginesie dyskusji o zakazie prewencyjnego badania trzeźwości pracowników dokonywanego samodzielnie przez pracodawcę pojawiło się ciekawe zagadnienie, dotyczące opinii sporządzanych przez IOD w odpowiedzi na pytania klientów, które daje pożywkę do dyskusji na temat funkcji i roli jaką pełni IOD w systemie prawa ochrony danych osobowych.

Z dużą dozą prawdopodobieństwa można założyć, że większość osób zajmujących się ochroną danych osobowych jest zgodna co do tego, że prewencyjne badanie trzeźwości pracowników dokonywane samodzielnie przez pracodawcę nie jest procesem przetwarzania szczególnie zagrażającym prawom i wolnościom osób, których dane dotyczą, a wprowadzenie tego rodzaju praktyki znacząco zmniejsza ryzyka wypadków przy pracy powodowanych przez pracowników będących pod wpływem alkoholu, co jest szczególnie istotne dla branży transportowej, ale także wielu przedsiębiorstw przemysłowych. Problem w powszechnym stosowaniu takiej praktyki jest taki, że pomiar alkomatem jest traktowany jako przetwarzanie danych dotyczących zdrowia danej osoby, a więc znajduje się w katalogu danych szczególnej kategorii z art. 9 RODO, co znacznie zawęża sytuacje, w których można takiego przetwarzania dokonywać. Poszukiwanie właściwej podstawy prawnej znacząco utrudnia lub uniemożliwia (tutaj możemy mówić o sporze w doktrynie i praktyce) stanowisko polskiego organu nadzorczego, w którym PUODO powołując się na przepisy kodeksu pracy oraz ustawy o wychowaniu w trzeźwości uważa, że nie ma obecnie podstaw prawnych do przeprowadzania takich badań samodzielnie przez pracodawców.

Mamy więc do czynienia z sytuacją, w której większość doktryny i praktyki uważa, że takie przetwarzanie jest możliwie na gruncie prawa ochrony danych, także uwzględniając cel, sposób przetwarzania, zasadę minimalizacji danych i ochronę interesów osób, których dane dotyczą, a organ nadzorczy ucina dyskusję wskazując, że dopóki nie zmieni się stan prawny to nie ma do tego podstaw, co oznacza wyraźny zakaz przeprowadzania takich badań.

Wymiar praktyczny tej sytuacji skupia się na odpowiedzi na pytanie, jaką opinię na temat przetwarzania danych osobowych w postaci dokonywania prewencyjnej kontroli trzeźwości powinna sporządzić dla administratora/procesora osoba pełniąca funkcję IOD? Różne odpowiedzi na to pytanie można zredukować do dwóch zasadniczych stanowisk, które występują w dyskusji w różnych wariacjach. Pierwsze z nich zakłada, że zadaniem IOD jest formułowanie opinii, dając bezwzględny prymat przepisom prawa ochrony danych osobowych oraz zaleceniom, uwagom i stanowiskom umocowanego ustawowo organu nadzorczego. Drugie stanowisko zakłada, że na opinię IOD wpływ powinny mieć nie tylko przepisy prawa ochrony danych, ale także powinna wynikać ona z rozpoznania szerszego kontekstu przetwarzania, brać pod uwagę ryzyka dotyczące administratora/procesora wynikające z innych gałęzi prawa czy mające swoje źródło w innych, niż przetwarzanie danych osobowych zjawiskach i procesach. W praktyce podejście pierwsze skutkuje zazwyczaj uznaniem, że osoba pełniąca funkcję IOD powinna negatywnie zaopiniować możliwość procesu prewencyjnej kontroli trzeźwości pracowników przez pracodawców, natomiast wedle drugiego stanowiska zapewnienie większego bezpieczeństwa życia i zdrowia, a także ograniczenie ryzyk innych, niż związanych z przetwarzaniem danych osobowych przeważa i powinno się takie przetwarzanie zaopiniować pozytywnie.

W tym miejscu warto powrócić do RODO i zastanowić się nad pozycją IOD. Zgodnie z art. 39 RODO na osobie pełniącej funkcję IOD ciążą m. in. obowiązek monitorowania przestrzegania prawa ochrony danych w organizacji, udzielanie zaleceń co do oceny skutków dla ochrony danych osobowych, ale także współpraca z organem nadzorczym, który na podstawie art. 57 RODO ma za zadanie m. in. monitorować i egzekwować stosowanie RODO, ale także upowszechniać wśród administratorów/procesorów wiedzę o obowiązkach spoczywających na nich na mocy RODO. Rodzi się więc pytanie o to, czy IOD realizując wspomniane obowiązki, w tym współpracę z organem



iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

nadzorczym, może sporządzić dla administratora/procesora opinię stojącą w sprzeczności z wyraźnym stanowiskiem organu nadzorczego.

Przyjmując podejście dające bezwzględny prymat prawu ochrony danych osobowych i współpracy z organem nadzorczym w formułowaniu opinii i wykonywaniu zadań IOD można argumentować, że obowiązkiem IOD jest upowszechnianie wśród administratorów/procesorów nie tylko treści przepisów RODO, ale także wszelkich stanowisk, zaleceń, poradników, wytycznych, decyzji oraz innych form wypowiedzi organu nadzorczego skierowanych do podmiotów stosujących rozporządzenie. Przywiązanie do treści RODO oraz wypowiedzi organu nadzorczego są często traktowane w dyskusji jako zarzut pod adresem IOD, rzekome ograniczenie w percepcji norm prawnych innych niż wynikających z RODO, zamknięcie się wyłącznie w przepisach o ochronie danych osobowych, czy wręcz wiązane jest z deficytem wiedzy na temat prawa czy specyfiki działalności danego administratora/procesora, gdy tymczasem jest to po prostu rzetelne wypełnianie obowiązków związanych z pełnieniem funkcji IOD, poruszanie się na podstawie i w granicach przepisów rozporządzenia regulujących obowiązki i sposób działania osób piastujących tą funkcję. Na potrzeby dyskusji nazwałbym takie podejście "kanonicznym".

Przyjmując podejście zakładające analizę szerszego spectrum regulacji i ocenę ryzyk pochodzących z różnych źródeł można argumentować, że IOD pełni przede wszystkim funkcję doradczą dla administratora/procesora, a różne formy wypowiedzi organu nadzorczego są po prostu opiniami na temat stosowania rozporządzenia, co do których IOD nie ma obowiązku się stosować i może formułować zalecenia i opinie dla administratora/procesora stojące z nimi w sprzeczności przedstawiając własną argumentację i analizę z założeniem, że i tak ewentualny spór z organem nadzorczym w tym zakresie rozstrzygnie sąd. Wyrazem przyjęcia tej koncepcji są stwierdzenia często padające w dyskusji "nie można się zamykać wyłącznie na RODO" czy "najgorsze to powiedzieć klientowi, że czegoś nie wolno, bo RODO".

Kuszące jest w tym miejscu okopać się na swoich pozycjach i ostrzeliwać się argumentami z teorii i praktyki oskarżając zwolenniczki/zwolenników podejścia "kanonicznego" o brak zrozumienia biznesu i wąskie horyzonty myślowe, a zwolenniczki/zwolenników myślenia "niekanonicznego" utratę niezależności i przedkładanie interesu klienta nad przestrzeganie RODO. Tymczasem sprawa nie jest taka prosta i oczywista, a poprowadzenie podziału po linii teoria vs praktyka fałszuje obraz sporu. Truizmem będzie stwierdzenie, że wszystko zależy od okoliczności, ale w praktyce faktycznie tak jest. Jeśli np. organizacja posiada oddzielny dział prawny, compliance, czy dział zajmujący się analizą ryzyka, a dodatkowo zatrudnia IOD z zewnątrz, to w tej sytuacji podejście "kanoniczne" będzie miało nie tylko walor niezachwianej wierności przepisom RODO, ale także głęboki sens praktyczny, bowiem opinia IOD ograniczona wyłącznie do zakresu ochrony danych osobowych stanie się elementem szerszej analizy stanu prawnego i oceny ryzyk. W podanym przykładzie prewencyjnej kontroli trzeźwości negatywna opinia IOD przedstawiająca stan prawny z uwzględnieniem stanowiska organu nadzorczego wskazująca na ryzyko kary i kontroli będzie ważnym elementem szerszej oceny, który zostanie zestawiony z oceną ryzyka wystąpienia wypadku i konsekwencji z tym związanych, szans na obronę swojego stanowiska w ewentualnym sporze i szacunkową oceną kosztów, które wiążą się ze spełnieniem ryzyka kontroli i kary lub ryzyka wystąpienia wypadku (taki model funkcjonowania IOD zdaje się być domyślny według RODO, biorąc pod uwagę wymóg powołania takiej funkcji i zapewnienie osobie ją piastującej niezależności). Uwzględnienie różnych ryzyk i szerszego ujęcia prowadzące do "zmiękczenia" argumentów z prawa ochrony danych może prowadzić do opinii nie oddającej w pełni rzeczywistego obrazu regulacji i ryzyk związanych z jej nieprzestrzeganiem, a w konsekwencji może zaburzyć proces decyzyjny. Nie można jednak zamykać oczu na praktykę i nie dostrzegać tego, że model współpracy gwarantujący pełną niezależność IOD i powierzenie tej funkcji osobie, która zajmie się wyłącznie tą jedną dziedziną dotyczy określonej grupy największych podmiotów, ale z pewnością nie jest dominujący na rynku. Często zdarza się, że IOD zajmuje się jednocześnie innymi zadaniami np. z zakresu compliance czy też szeroko rozumianą obsługą prawną podmiotu. W takiej sytuacji bardziej naturalne (i często właściwe) będzie szersze spojrzenie na stan prawny przed sformułowaniem opinii, bowiem obok ryzyka związanego z ewentualną kontrolą czy karą ze strony organu nadzorczego istnieją inne ryzyka, które



iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

mogą nieść jeszcze większe konsekwencje w przypadku ich ziszczenia. W takiej sytuacji zrozumiałe będzie zajęcie stanowiska przedkładające całokształt sytuacji prawnej nad ograniczenie się tylko do prawa ochrony daych osobowych, choć warto się zastanowić, czy takie podejście będzie naruszeniem niezależności IOD, co nie jest tylko pytaniem teoretycznym od czasu decyzji belgijskiego organu nadzorczego, który wskazał na naruszenie zasady niezależności IOD w przypadku, gdy osoba pełniącą tą funkcję była też odpowiedzialna za compliance, analizę ryzyka i audyty.

Podsumowując ten wywód można założyć, że jesteśmy dopiero na początku dyskusji na temat pozycji IOD i modelowego zachowania w sytuacji pewnej sprzeczności pomiędzy opinią opartą wyłącznie na prawie ochrony danych osobowych i wypowiedziach organu nadzorczego, a opiniami opartymi o szerszą podstawę prawną. Nie ulega wątpliwości, że temat będzie powracał przy różnych okazjach, a spór zdaje się mieć na tyle systemowe podłoże związane z funkcjonującymi modelami współpracy IOD z administratorami/procesorami, że nie zostanie szybko rozstrzygnięty poprzez przekonanie jednych przez drugich. Intuicja podpowiada, że organ nadzorczy nie będzie specjalnie nadgorliwy w przecinaniu takich dyskusji usuwaniem sprzeczności i rozjaśnianiem podstaw, na których są oparte, a więc w najbliższym czasie będziemy musieli się nauczyć żyć z tą rozbieżnością pomiędzy podejściem "kanonicznym", a "niekanonicznym". Dla przejrzystości dyskusji pewnie warto będzie na przyszłość precyzować ,z jakich pozycji i okoliczności wyprowadza się własne tezy oraz dbać o to, aby dyskusja nie przerodziła się w licytację o zawartość IODa w IODzie. W kwestii komunikacji IOD z administratorami/procesorami pozostaje jedynie zamknąć temat w stylu linkedinowego Paulo Coelho - najważniejsza jest szczera i przejrzysta komunikacja własnych stanowisk.

**Bartosz Migas,**
**Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.**



iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł