8. Sprawy dotyczące ochrony danych osobowych.

W sprawie o **sygn. akt II SA/Wa 736/08** Wojewódzki Sad Administracyjny w Warszawie wyrokiem z dnia 19 sierpnia 2008 r. uchylił zaskarżoną decyzję i decyzję ją poprzedzającą.

Zaskarżoną decyzją Generalny Inspektor Ochrony Danych Osobowych utrzymał w mocy swą wcześniejszą decyzję, którą nakazał Polskiej Agencji Rozwoju Przedsiębiorczości, jako administratorowi danych beneficjentów ostatecznych przetwarzanych w związku z realizacją działania 2.3 Sektorowego Programu Operacyjnego Rozwój Zasobów Ludzkich 2004 - 2006 (SPO RZL 2004-2006), usunięcie uchybień w procesie przetwarzania danych osobowych poprzez: 1) zapewnienie, aby system informatyczny o nazwie „P" (służący do przetwarzania danych osobowych beneficientów ostatecznych) umożliwiał, dla każdej osoby, odnotowanie informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, 2) zapewnienie, aby system informatyczny o nazwie „P" umożliwiał, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, tj. o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

Istota sporu i zarazem podstawowy zarzut skargi sprowadza się do sposobu interpretacji pojęcia administrator danych w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, w sytuacji gdy dane osobowe są przetwarzane przez co najmniej dwa podmioty z sektora publicznego, a cele i środki przetwarzania tych danych wynikają z powszechnie obowiązujących przepisów prawa.

W ocenie Sądu, Polska Agencja Rozwoju Przedsiębiorczości przetwarzając dane osobowe beneficjentów ostatecznych nie działała jako administrator danych

osobowych, lecz jako przetwarzający te dane w ramach umowy zawartej z administratorem danych, o której mowa w art. 31 ustawy o ochronie danych osobowych. Świadczą o tym bowiem szczegółowe postanowienia dwóch zawartych na piśmie umów pomiędzy instytucją zarządzającą – Ministrem Gospodarki i Pracy (a następnie Ministrem Rozwoju Regionalnego) – a instytucją wdrażającą – Polską Agencją Rozwoju Przedsiębiorczości.

Według Sądu, to Minister Gospodarki i Pracy, a potem Minister Rozwoju Regionalnego zawierając powyższe umowy występował jako administrator danych, a okoliczność ta wynika z faktu, że to Minister jako instytucja zarządzająca konkretyzował cele i środki przetwarzania danych osobowych beneficjentów ostatecznych, będąc odpowiedzialnym tak za przygotowanie sektorowego programu operacyjnego, jak i jego realizację.

Przede wszystkim to Minister korzystał z przewidzianych w art. 18 ustawy o Narodowym Planie Rozwoju kompetencji i realizując Program Operacyjny wydawał Polskiej Agencji Rozwoju Przedsiębiorczości wytyczne.

W konsekwencji, w ocenie Sądu, adresatem decyzji Generalnego Inspektora Ochrony Danych Osobowych nakazującej przywrócenie stanu zgodnego z prawem mogła być PARP, ale występująca w sprawie jako przetwarzający dane osobowe na podstawie umowy, a nie jako administrator tych danych, a możliwość taką przewiduje wprost ustawa o ochronie danych w art. 18 w zw. z art. 31 ust. 3 i 5.

Jednocześnie Sąd stwierdził, że czym innym jest właściwe ustalenie adresata decyzji, a czym innym zapewnienie stronie czynnego udziału w postępowaniu administracyjnym. Z analizy akt postępowania wynika, że organ nie zapewnił Ministrowi Rozwoju Regionalnego udziału na żadnym etapie postępowania.

W rezultacie administrator danych nie mógł występować w postępowaniu w obronie własnego interesu prawnego dotyczącego ciążącej na nim odpowiedzialności w sytuacji umownego powierzenia przetwarzania danych innemu podmiotowi (art. 31 ust. 4 ustawy o ochronie danych), a tym samym w postępowaniu wystąpiło naruszenie prawa dające podstawę do jego wznowienia (art. 145 § 1 pkt 4 kpa), co uzasadniało uchylenie zaskarżonej decyzji i decyzji ją poprzedzającej.

Wyrokiem z dnia 27 listopada 2008 r., **sygn. akt II SA/Wa 903/08**, Wojewódzki Sąd Administracyjny w Warszawie uchylił decyzję Generalnego Inspektora Ochrony Danych Osobowych oraz utrzymaną nią w mocy decyzje tego organu, którą nakazano Spółce L. usunięcie uchybień w procesie przetwarzania danych poprzez usunięcie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Spółki oraz zaprzestanie zbierania tych danych osobowych.

Odwołując się do definicji danych osobowych, Sąd stwierdził, że linie papilarne z uwagi na swą niepowtarzalność stanowią cechę fizyczną osoby, umożliwiającą jej identyfikację i jako takie tworzą szerszą grupę danych biometrycznych, mających walor danych osobowych, w rozumieniu art. 6 ustawy o ochronie danych osobowych (podobnie jest w przypadku wzoru siatkówki oka).

WSA w Warszawie wskazał, że dane biometryczne w postaci odcisków linii papilarnych palców pracowników zostały uzyskane na podstawie zgody, wyrażonej przez pracownika w postaci pisemnego oświadczenia. Co stanowiło przesłankę legalności przetwarzania określoną art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

Sąd nie zgodził się ze stanowiskiem organu, że do przedmiotowego stanu faktycznego nie znajdują zastosowania przepisy prawa, które zezwalałyby na przetwarzanie innych danych osobowych pracowników w celu prowadzenia ewidencji czasu pracy niż dane wymienione w art. 22^1 § 1 i 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (t. j.: Dz. U. z 1998 r. Nr 21, poz. 94 ze zm.).

Dokonując wykładni przepisu art. 22^1 kp, Sąd wskazał, że wprawdzie w § 1-4 tego przepisu nie ma mowy o danych osobowych pracownika w postaci linii papilarnych, nie zmienia to jednak faktu, że – poprzez art. 22^1 § 5 kp – pracodawca może gromadzić także i tego rodzaju dane, o ile spełniona zostanie choćby jedna z przesłanek legalizujących ich przetwarzanie. Za taką zaś przesłankę Sąd uznał pisemną zgodę pracowników Spółki (art. 23 ust. 1 ustawy o ochronie danych osobowych). Wyrok nie jest prawomocny.

Kwestia przetwarzania określonej kategorii danych osobowych i przesłanek legalizujących ich przetwarzanie była także przedmiotem oceny Sądu w wyroku z dnia

23 kwietnia 2008 r., **sygn. akt II SA/Wa 1552/06** (wyrok nieprawomocny). Sąd, wyrokiem tym, uchylił decyzje Generalnego Inspektora Ochrony Danych Osobowych, którymi nakazano jednemu z operatorów telefonii komórkowej udostępnienie Komendantowi Straży Miejskiej w W. danych osobowych abonenta – domniemanego sprawcy wykroczenia - posługującego się określonym numerem telefonu.

W ocenie Sądu ani art. 11 określający zadania straży miejskiej, ani art. 12 ust. 1 pkt 5 określający uprawnienia strażnika miejskiego, ani też art. 10a określający zakres danych osobowych, do którego przetwarzania uprawniona jest straż miejska nie stanowią przesłanki legalizującej przetwarzanie danych telekomunikacyjnych abonenta.

WSA w Warszawie zaznaczył, że odmienne stanowisko stanowiłoby jaskrawe zaprzeczenie zasadzie legalizmu, gdyż w ustawie o strażach gminnych, w odróżnieniu od ustawy o Policji, ustawy o Straży Granicznej, ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, czy ustawy o Wojskowych Służbach Informacyjnych, nie przewidziano środków i uprawnień do przetwarzania owych danych.

Podkreślił także, że uprawnienia Straży Miejskiej w zakresie prawa dostępu do danych objętych tajemnicą telekomunikacyjną nie wynikają również z odrębnych przepisów, o których mowa w pkt 2 art. 10a ustawy o strażach gminnych. Zatem, skoro dla tej formacji nie przewidziano dostępu do tajemnicy telekomunikacyjnej zarówno w ustawie o strażach gminnych, jak i w odrębnych przepisach, to powoływanie się na dobro publiczne w rozumieniu art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych, jest niedopuszczalne z tego powodu, że w demokratycznym państwie prawa, organy władzy publicznej obowiązane są do działania na podstawie i w granicach prawa (art. 7 Konstytucji Rzeczypospolitej Polskiej i art. 6 Kodeksu postępowania administracyjnego).

Sąd stwierdził, że wykładnia celowościowa ostatniego zdania art. 161 Prawa telekomunikacyjnego, nie przemawia za możliwością udostępniania tajemnicy telekomunikacyjnej na podstawie art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych. Zauważył ponadto, że zdanie owo stanowi transpozycję art. 15 ust. 1 Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze

łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), (Official Journal L 201, 31/07/2002, s. 37). Wynika z niego, że państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia między innymi poufności komunikacji (art. 5 Dyrektywy), gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej.

Dodatkowo Sąd podniósł, że niezasadnym wydaje się powoływanie w niniejszej sprawie na klauzulę bezpieczeństwa publicznego (art. 15 ust. 1 Dyrektywy 2002/58/WE) ze względu na sposób jego rozumienia w prawie europejskim. W prawie europejskim bowiem odwołanie się do tej klauzuli jest możliwe wówczas, gdy zaistnieje rzeczywiste i dostatecznie poważne zagrożenia podstawowego interesu społecznego. Sąd wskazał przy tym zgodny z tym stanowiskiem wyrok ETS z dnia 14 marca 2000 r. w sprawie C-54/99 oraz fragment opinii Rzecznika Generalnego Juliane Kokott przedstawionej w dniu 18 lipca 2007 r. do sprawy o sygn. C-275/06.

Z tych też względów Sąd nie uznał, aby w rozpoznawanej sprawie czyn określony w art. 63a Kodeksu wykroczeń będący przedmiotem postępowania prowadzonego przez Straż Miejską świadczył o poważnym zagrożenie podstawowego interesu społeczeństwa i uzasadniał zarazem udostępnienie danych objętych tajemnicą telekomunikacyjną względami bezpieczeństwa.