Sygn. akt II SA/Wa 2129/20

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 13 maja 2021 r.

Wojewódzki Sąd Administracyjny w Warszawie
w składzie następującym:

Przewodniczący Sędzia WSA	Joanna Kube
Sędzia WSA	Ewa Radziszewska-Krupa
Sędzia WSA	Karolina Kisielewicz (spr.)

po rozpoznaniu na posiedzeniu niejawnym w dniu 13 maja 2021 r.
sprawy ze skargi Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie
na decyzję Prezesa Urzędu Ochrony Danych Osobowych
z dnia 21 sierpnia 2020 r. nr ZSOŚS.421.25.2019.88353
w przedmiocie przetwarzania danych osobowych

oddala skargę

Sygn. akt II SA/Wa 2129/20

UZASADNIENIE

Szkoła Głowna Gospodarstwa Wiejskiego z siedzibą w Warszawie zaskarżyła do Wojewódzkiego Sądu Administracyjnego w Warszawie decyzję Prezesa Urzędu Ochrony Danych Osobowych z 21 sierpnia 2020 r. (nr ZSOŚS.421.25.2019.88353), którą organ działając na podstawie art. 104 § 1 k.p.a., art. 7 ust. 1, art. 60, art. 102 ust. 1 i ust. 3 ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz art. 57 ust. 1 lit. a, art. 58 ust. 2 lit. d oraz lit. i w zw. z art. 5 ust. 1 lit. e i lit. f, art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b. i lit. d, art. 32 ust. 2, art. 38 ust. 1, art. 39 ust. 1 lit. b i art. 39 ust. 2, art. 30 ust. 1 lit. d, i art. 83 ust. 1 - 3, art. 83 ust. 4 lit a i art. 83 ust. 5 lit. a rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.) stwierdził naruszenie przez skarżącą przepisów art. 5 ust. 1 lit. e, art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d, art. 32 ust. 2, art. 38 ust. 1, art. 39 ust. 1 lit. b i art. 39 ust. 2 rozporządzenia RODO i nałożył na skarżącą karę pieniężną w wysokości 50.000 zł oraz w pozostałym zakresie postępowanie umorzył.

W uzasadnieniu tej decyzji organ podał, że Szkoła Główna Gospodarstwa Wiejskiego w Warszawie dokonała zgłoszenia Prezesowi Urzędu Ochrony Danych osobowych faktu naruszenia ochrony danych osobowych kandydatów na studia w SGGW.

Od listopada do listopada 2019 r. dokonano czynności kontrolnych w Szkole Głównej Gospodarstwa Wiejskiego w Warszawie. Zakresem kontroli objęto przetwarzanie przez Szkołę Główną Gospodarstwa Wiejskiego w Warszawie danych osobowych osób, których dotyczy naruszenie ochrony danych osobowych, zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych.

Stan faktyczny ustalony podczas kontroli szczegółowo opisano w protokole kontroli, który został podpisany przez rektora SGGW.

Na podstawie zgromadzonego w sprawie materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych kandydatów na studia w SGGW,

Uczelnia jako administrator, naruszyła przepisy o ochronie danych osobowych. Naruszenie przepisów polegało na:

1) dokonaniu w sposób niewystarczający przez administratora oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych kandydatów, co stanowi naruszenie art. 5 ust. 1 lit. e, art. 5 ust. 1 lit f, art. 5 ust. 2, art. 24 ust. 1, art. 25 ust 1, art. 32 ust. 1 lit b, art. 32 ust. 1 lit. d, art. 32 ust. 2 i art. 38 ust. 1 rozporządzenia 2016/679;

2) nieuwzględnianiu w sposób wystarczający przez administratora, przy korzystaniu z systemu służącego do przetwarzania danych osobowych kandydatów, zasady rozliczalności, co stanowi naruszenie art. 5 ust. 2 rozporządzenia 2016/679;

3) wypełnianiu przez inspektora ochrony danych zadań bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania, co stanowi naruszenie art. 24 ust. 1, art. 32 ust. 1, art. 32 ust. 2, art. 38 ust. 1, art. 39 ust. 1 lit. b i art. 39 ust. 2 rozporządzenia 2016/679;

4) nieuwzględnieniu w prowadzonym w SGGW rejestrze czynności przetwarzania danych osobowych, w zakresie czynności przetwarzania danych osobowych kandydatów na studia pierwszego, drugiego stopnia i jednolitych studiów magisterskich w SGGW wszystkich wymaganych przepisami rozporządzenia 2016/679 informacji, co stanowi naruszenie art. 30 ust. 1 lit. d rozporządzenia 2016/679.

Ustalono, że naruszenie ochrony danych osobowych kandydatów na studia w SGGW, które miało miejsce listopada 2019 r., związane było z kradzieżą przenośnego prywatnego komputera pracownika SGGW A G - adiunkta w Katedrze , pełniącego również funkcję sekretarza Uczelnianej Komisji Rekrutacyjnej SGGW. Skradziony laptop był używany przez tego pracownika do celów prywatnych i służbowych, w tym również do przetwarzania danych osobowych kandydatów na studia w SGGW na potrzeby czynności rekrutacyjnych w ramach pełnionej funkcji sekretarza Uczelnianej Komisji Rekrutacyjnej. Z Systemu Obsługi Kandydatów służącego do przetwarzania danych osobowych kandydatów na studia I i II stopnia oraz jednolitych studiów magisterskich (zwanym dalej także: „SOK") za pomocą zaimplementowanej w nim funkcjonalności, importował na swój prywatny komputer zestawy danych osobowych, obejmujących m.in. imię, nazwisko, nazwisko rodowe, imiona rodziców, numer identyfikacyjny PESEL, płeć, narodowość, obywatelstwo,

adres zamieszkania, serię i numer dowodu osobistego bądź innego dokumentu tożsamości, w tym paszportu, numer telefonu komórkowego i/lub stacjonarnego, informacje o dotychczasowym wykształceniu, informacje o kwalifikacji na studia. Uczelnia, będąca administratorem tych danych osobowych, nie posiadała informacji o tym fakcie. Operacja ta również nie była rejestrowana w SOK. A G pobrane zestawy danych przygotowywał do kwalifikacji poprzez ich odpowiednie filtrowanie w arkuszu kalkulacyjnym według odpowiednich kryteriów kwalifikacyjnych, które są określone dla poszczególnych kierunków studiów, a następnie przedstawiał na spotkaniu kwalifikacyjnym komisji rekrutacyjnej. Na podstawie pobranych zestawów danych osobowych pan A G sporządzał również raporty końcowe z zestawieniami statystycznymi według wybranych kryteriów. Na skradzionym komputerze miał założony katalog z rekrutacją na konkretny rok, w którym przechowywał różne pliki raportowo-bazowe, a także inne dokumenty, jak np. odpowiedzi na pisma w sprawach związanych z rekrutacją.

Naruszenie ochrony danych osobowych dotyczy kandydatów na studia w SGGW z okresu ostatnich lat i z przeprowadzonych przez Uczelnię obliczeń wynika, że obejmuje 81 624 rekordy (wpisy) w Systemie Obsługi Kandydatów.

W związku z powyższym, pismem z marca 2020 r. Prezes UODO wszczął z urzędu postępowanie administracyjne w zakresie stwierdzonych uchybień, w celu ustalenia zgodności przetwarzania danych osobowych kandydatów na studia w SGGW z przepisami o ochronie danych osobowych.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, rektor SGGW złożył wyjaśnienia i podjął polemikę z ustaleniami i ocenami organu.

Organ po zapoznaniu się z tymi wyjaśnieniami i rozważeniu całego zgromadzonego materiału dowodowego uznał jednak, że Uczelnia w sposób niewystarczający dokonywała oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych kandydatów na studia, co stanowi naruszenie art. 5 ust. 1 lit. e, art, 5 ust. 1 lit. f, art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d, art. 32 ust. 2 i art. 38 ust. 1 rozporządzenia 2016/679, w tym nie uwzględniała w sposób wystarczający zasady rozliczalności korzystając z systemu informatycznego służącego do przetwarzania danych osobowych kandydatów na studia, co stanowi naruszenie art. 5 ust. 2 rozporządzenia 2016/679.

W rozwinięciu tych zarzutów naruszenia prawa przez Uczelnię przytoczył treść przepisów rozporządzenia 2016/679, które zdaniem organu zostały naruszone, przedstawił zadania i obowiązki administratora danych osobowych z tych przepisów wynikające oraz ich naruszenia przez skarżącą Uczelnię.

Prezes UODO zarzucając niewystarczającą ocenę zastosowanych środków technicznych i organizacyjnych obejmujących proces przetwarzania danych osobowych kandydatów na studia w SGGW kierował się zasadą wynikającą z art. 24 ust 1 rozporządzenia 2016/679 jaką jest kontrola administratora nad procesami przetwarzania danych osobowych.

O braku zastosowania się do tej zasady oraz braku nadzorowania przez administratora przestrzegania przez pracownika SGGW zasad przetwarzania danych obowiązujących na Uczelni świadczy wykorzystywanie przez pracownika SGGW prywatnego urządzenia do przetwarzania danych kandydatów na studia w SGGW z okresu ostatnich lat, brak wiedzy administratora o tym fakcie, możliwość pobierania danych tych osób z systemu SOK bez rejestrowania tego procesu w tym systemie informatycznym i gromadzenie ich przez pracownika poza obszarem przetwarzania, wbrew przyjętym procedurom, A G działania te podejmował poza zakresem upoważnienia, gdyż za każdym razem upoważnienie obejmowało dane osobowe objęte rekrutacją na studia na dany rok akademicki, zarówno tych przetwarzanych na nośnikach papierowych, jak i tych przetwarzanych w systemie SOK. Upoważnienie nie obejmowało zapisywania i przechowywania danych osobowych na prywatnym komputerze i wynoszeniu ich poza teren SGGW. Jednocześnie, jak wynika z materiału zgromadzonego w toku kontroli, Uczelnia ograniczyła się do odebrania od pracownika oświadczenia o zachowaniu danych osobowych w tajemnicy i o zapoznaniu się z systemem ochrony danych osobowych obowiązującym na Uczelni. Nie kontrolowała jednak przetwarzania danych osobowych w związku z czynnościami służbowym wykonywanymi przez pracownika. Na administratorze ciąży zaś obowiązek zweryfikowania w organizacji obszarów przetwarzania danych osobowych i wdrożenia odpowiednich środków technicznych i organizacyjnych mających zapewnić ich bezpieczeństwo.

Z materiału dowodowego zgromadzonego w toku kontroli, jak i z powyższych wyjaśnień złożonych w toku postępowania administracyjnego, nie wynika by Uczelnia dokonała oceny ryzyka w zakresie możliwości naruszenia zasady poufności danych osobowych (art. 5 ust. 1 lit. f rozporządzenia 2016/679) czy zasady ograniczenia

przechowywania danych (art. 5 ust. 1 lit. e rozporządzenia 2016/679), wynikającego z zagrożenia jakim jest możliwość eksportowania z systemu SOK szerokiego zakresu kategorii danych osobowych na nośnik zewnętrzny. Administrator poprzestał na tych dokumentach podpisanych przez pracownika i wdrożeniu środków organizacyjnych w postaci Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych.

W związku z tym zdaniem organu, Uczelnia naruszyła art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b i lit. d oraz art. 32 ust. 2 rozporządzenia 2016/679 poprzez wdrożenie w sposób niewystarczający środków technicznych i organizacyjnych, które powinny podlegać regularnym przeglądom i aktualizacji biorąc pod uwagę czynniki i okoliczności dotyczące przetwarzania danych osobowych wskazane w tym przepisie. Wdrożenie odpowiednich środków ma na celu realizację jednej z ogólnych zasad przetwarzania danych - zasady integralności i poufności, określonej w art. 5 ust. 1 lit. f rozporządzenia 2016/679, która w konsekwencji również została przez administratora naruszona. Ponadto z art. 24 ust. 1 rozporządzenia 2016/679 wynika obowiązek wykazania spełnienia wymogów dotyczących zabezpieczenia danych i zgodności z przepisami rozporządzenia, co przejawia się w dokumentowaniu działań podjętych w celu zapewnienia zgodności z przepisami rozporządzenia i nawiązuje do zasady rozliczalności określonej w art. 5 ust. 2 rozporządzenia 2016/679. W zebranym w postępowaniu materiale brak jest dowodów potwierdzających nadzorowanie przez administratora przestrzegania przez pracownika SGGW A G zasad przetwarzania danych osobowych określonych w dokumentach obowiązujących na Uczelni oraz rozporządzeniu 2016/679, wobec czego zasadny jest także zarzut naruszenia art. 5 ust. 2 rozporządzenia 2016/679. Monitorowanie polityki w dziedzinie ochrony danych osobowych należy do obowiązków administratora, a także inspektora ochrony danych, który ma za zadanie wspierać administratora w przestrzeganiu przepisów o ochronie danych osobowych.

Ponadto na podstawie zebranego w toku kontroli materiału dowodowego. Prezes UODO stwierdził, że nie został przeprowadzony audyt wewnętrzny obejmujący poszczególne jednostki organizacyjne SGGW oraz że inspektor ochrony danych nie przeprowadzał analizy ryzyka związanej z przetwarzaniem danych osobowych kandydatów na studia w SGGW. Nie informował on też o konieczności jej sporządzenia przez rektora SGGW czy kierownika Biura Spraw Studenckich, który

zgodnie z strukturą organizacyjną Uczelni odpowiada za proces rekrutacji na studia w SGGW. Audyty związane z operacjami przetwarzania danych nie były przeprowadzane przez inspektorów ochrony danych w sposób kompleksowy.

Art. 38 rozporządzenia 2016/679 nakłada na administratora bezwzględny obowiązek właściwego i niezwłocznego włączania inspektora ochrony danych we wszystkie sprawy dotyczące ochrony danych osobowych. Uczelnia dopuściła się naruszenia tego przepisu nie włączając inspektora ochrony danych osobowych w sprawy dotyczące ochrony danych osobowych w zakresie przyjmowanych rozwiązań technicznych w ramach funkcjonowania systemu SOK.

Dowody zgromadzone w sprawie pozwalają stwierdzić, że Uczelnia mimo świadomości istnienia w procesie przetwarzania danych osobowych kandydatów na studia, technicznej możliwości przetwarzania polegającego na eksportowaniu na zewnętrzny nośnik danych osobowych z systemu informatycznego z uwagi na funkcjonalność umożliwiającą niekontrolowany eksport szerokiego zakresu danych osobowych z systemu SOK i świadomości w tym zakresie Biura Spraw Studenckich, zignorowała to zagrożenie. Nie podejmowała weryfikacji tej operacji przetwarzania, o czym świadczy fakt przetwarzania danych osobowych przez pracownika Uczelni z okresu ostatnich lat rekrutacji na studia w SGGW na prywatnym komputerze.

To wszystko świadczy o tym, że Uczelnia nie podjęła działań mających na celu zapewnienie monitorowania poziomu zagrożeń oraz rozliczalności w tym zakresie, a także adekwatności wprowadzonych zabezpieczeń. W związku z powyższym zasadny jest zarzut naruszenia przez SGGW w tym zakresie art. 24 ust. 1, 32 ust. 1 lit. d i art. 32 ust. 2 rozporządzenia 2016/679 w związku z art. 5 ust. 2 rozporządzenia 2016/679. Stanowi również o naruszeniu art. 32 ust. 1 lit. b w związku z art. 5 ust. 1 lit. f rozporządzenia 2016/679, przez brak wdrożenia przez administratora odpowiednich środków technicznych i organizacyjnych, w celu zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzania danych osobowych kandydatów na studia w SGGW w zakresie zdolności do ciągłego zapewnienia poufności przetwarzania.

Przechowywanie przez pracownika Uczelni, A G , danych osobowych kandydatów na studia w SGGW, pochodzących z okresu ostatnich lat rekrutacji, w wyniku wykonywanych czynności służbowych jest wreszcie niezgodne z wyznaczonym okresem przechowywania danych osobowych

kandydatów na studia, który został określony w SGGW na 3 miesiące od zakończenia rekrutacji, co stanowi naruszenie przez administratora art. 25 ust. 1 rozporządzenia 2016/679 w związku z art. 5 ust. 1 lit. e rozporządzenia 2016/679, tj. poprzez nieuwzględnienie odpowiednich środków technicznych i organizacyjnych w celu skutecznej realizacji zasady ograniczenia przechowywania, zwaną także zasadą czasowego ograniczenia przetwarzania danych.

Uczelnia dopuszczając taki stan rzeczy nie uwzględniła w sposób wystarczający zasady rozliczalności określonej art. 5 ust. 2 rozporządzenia 2016/679. Administrator powinien bowiem móc wykazać, że osoby, które upoważnił do przetwarzania danych osobowych przetwarzają je zgodnie z zasadami określonymi w rozporządzeniu 2016/679, tj. tylko wtedy, kiedy jest to niezbędne dla uzyskania określonego celu przetwarzania oraz w zakresie jakim jest to niezbędne.

Zasada rozliczalności określona w art. 5 ust. 2 rozporządzenia 2016/679 została uszczegółowiona w art. 24 ust. 1 i art. 32 ust. 1 tego rozporządzenia, który nakłada na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

Zgodnie z art. 38 ust. 1 rozporządzenia 2016/679 administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Jak już Prezes UODO wskazał, inspektor ochrony danych osobowych nie był angażowany w proces rekrutacji na studia obejmujący funkcjonowanie systemu informatycznego przeznaczonego do tego procesu.

Jedną z osób zaangażowanych w proces przetwarzania danych osobowych na Uczelni podczas rekrutacji kandydatów na studia jest A G Prezes UODO ustalił, że A G nie brał udziału w szkoleniu dotyczącym ochrony danych osobowych w procesie ich przetwarzania, w żadnym z wyznaczonych terminów tych szkoleń. Administrator powinien podjąć skuteczne działania w celu zapewnienia przeszkolenia tej osoby w zaplanowanym zakresie poprzez dobór odpowiedniej formy kształcenia. Mając na uwadze powyższe oraz treść art. 24 ust. 1 i art. 32 ust. 1 i 2 rozporządzenia 2016/679, obligujących administratora do wdrożenia odpowiednich środków organizacyjnych i technicznych, organ stwierdził, że administrator nie wypełnił tego obowiązku należycie.

W związku z tym Uczelnia dopuściła się również naruszenia art. 39 ust. 1 lit. b rozporządzenia 2016/679 poprzez nieuwzględnienie faktu nieuczestniczenia A G w zaplanowanych szkoleniach i art. 39 ust. 2 rozporządzenia 2016/679 poprzez niepotraktowanie tej okoliczności jako czynnika wskazującego na konieczność zweryfikowania, czy z tego tytułu A G w sposób prawidłowy i zgodny z procedurami przyjętymi na Uczelni dokonuje przetwarzania danych osobowych w ramach swoich obowiązków służbowych, mając na względzie pełnioną przez niego szczególną funkcję - sekretarza Uczelnianej Komisji Rekrutacyjnej oraz zakres powierzonych mu w związku z tym obowiązków.

Na podstawie wyżej przedstawionych ustaleń Prezes Urzędu Ochrony Danych Osobowych, korzystając z przysługującego mu uprawnienia określonego w art. 58 ust. 2 lit. i rozporządzenia 2016/679, zgodnie z którym każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych przewidzianych w art. 58 ust. 2 lit. a-h oraz lit. j tego rozporządzenia, administracyjnej kary pieniężnej na mocy art. 83 rozporządzenia 2016/679, mając na względzie okoliczności ustalone w postępowaniu stwierdził, że w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na Uczelnię administracyjnej kary pieniężnej.

Nakładając tę karę organ - stosownie do treści art. 83 ust. 2 lit. a-k rozporządzenia 2016/679 - wziął pod uwagę następujące okoliczności sprawy, wpływające obciążająco i mające wpływ na wymiar nałożonej kary finansowej:

1. Waga i charakter naruszeń - przy wymierzaniu kary istotne znaczenie miała okoliczność, że naruszenie ochrony danych osobowych dotyczy kandydatów na studia w SGGW z okresu ostatnich 5 lat oraz że liczba osób dotkniętych naruszeniem wynosi 100 000 jako górna granica
2. Prezes UODO wziął pod uwagę, że naruszenie ochrony danych było skutkiem używania przez pracownika niezabezpieczonego prywatnego komputera przenośnego do celów prywatnych i służbowych, w tym również do przetwarzania danych osobowych kandydatów na studia w SGGW na potrzeby czynności rekrutacyjnych w ramach pełnionej funkcji sekretarza w Uczelnianej Komisji Rekrutacyjnej, przy jednoczesnym braku wiedzy administratora o tym fakcie i niekontrolowaniu tego procesu również w systemie SOK poprzez brak rejestrowania operacji pobierania danych osobowych z tego systemu informatycznego.

3. Kategorie danych osobowych, których dotyczyło naruszenie ochrony danych osobowych - System Obsługi Kandydatów, w związku z zaimplementowaną w tym systemie funkcjonalnością, umożliwiał importowanie na komputer prywatny, użytkowany przez sekretarza Uczelnianej Komisji Rekrutacyjnej i wykorzystywany także do wykonywania czynności służbowych, zestawu danych kandydatów na studia I i II stopnia oraz jednolitych studiów magisterskich w SGGW obejmujących: imię, nazwisko, nazwisko rodowe, imiona rodziców, numer identyfikacyjny PESEL, płeć, narodowość, obywatelstwo, adres zamieszkania, serię i numer dowodu osobistego bądź innego dokumentu tożsamości, w tym paszportu, numer telefonu komórkowego i/lub stacjonarnego oraz inne kategorie danych dotyczące dotychczasowego przebiegu nauczania: tj. informacja o ukończonej szkole średniej, dane szkoły średniej w tym miejscowość, rok ukończenia szkoły średniej, numer i data świadectwa ukończenia szkoły średniej, organ wydający świadectwo, rok matury i data świadectwa maturalnego, organ wydający świadectwo maturalne, wyniki uzyskane na egzaminie maturalnym, ukończone studia, ukończona uczelnia, ukończony kierunek studiów, ocena na dyplomie, średnia ocen ze studiów, kierunek studiów, o który kandydat się ubiega, informacja o zakwalifikowaniu na studia, punkty kwalifikacyjne kandydata, zbieżność kierunku studiów ukończonego z tym, o który się kandydat ubiega (pełen wykaz kategorii danych osobowych, dla poszczególnych raportów, dostępnych w ramach funkcjonalności umożlwiającej eksport danych stanowi załącznik nr 59 do protokołu kontroli). W ten sposób niewątpliwie doszło do naruszenia szerokiego zakresu danych osobowych kandydatów na studia w SGGW, co stanowi istotną okoliczność wpływającą na wysokość kary administracyjnej.

4. Czas trwania naruszeń - dane osobowe kandydatów na studia w SGGW w formie umożliwiającej identyfikację osoby, której dane dotyczą, przechowywane były przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

A G - sekretarz Uczelnianej Komisji Rekrutacyjnej przechowywał dane osobowe kandydatów na studia w SGGW pochodzące z okresu ostatnich lat rekrutacji na przenośnym prywatnym komputerze, co było niezgodne z wyznaczonym okresem przechowywania danych osobowych kandydatów na studia, który został określony w SGGW na 3 miesiące od zakończenia rekrutacji.

5. Wysoki stopień odpowiedzialności administratora - ustalenia dokonane przez Prezesa Urzędu Ochrony Danych Osobowych pozwalają na stwierdzenie, że od początku stosowania rozporządzenia 2016/679, w ramach procesu przetwarzania

danych osobowych kandydatów na studia w SGGW administrator nie stosował się do podstawowych zasad dotyczących przetwarzania danych osobowych, określonych w tym rozporządzeniu.

W uzasadnieniu zaskarżonej decyzji organ podał również okoliczności łagodzące mające wpływ na wymiar kary. Uwzględnił:

1. Podjęcie przez SGGW wszelkich możliwych działań, mających na celu usunięcie naruszenia;
2. Działania podjęte następczo w stosunku do naruszenia mające na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych w SGGW w przyszłości;
3. Dobrą współpracę ze strony Uczelni, która zarówno w toku przeprowadzonej kontroli, jak i w trakcie trwania postępowania administracyjnego współpracowała z Prezesem Urzędu Ochrony Danych Osobowych w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków; w wyznaczonym terminie Uczelnia przesłała wyjaśnienia i udzieliła odpowiedzi na wystąpienie Prezesa Urzędu Ochrony Danych Osobowych, zatem stopień tej współpracy należy ocenić jako pełny;
4. Brak dowodów, aby osoby, których dane dotyczą, doznały szkody majątkowej, niemniej już samo naruszenie poufności danych stanowi szkodę niemajątkową (krzywdę);
5. Fakt, że Uczelnia nie dopuściła się uprzednio naruszenia przepisów rozporządzenia 2016/679, które miałoby istotne znaczenie dla niniejszego postępowania.

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie w skardze wniesionej do Wojewódzkiego Sądu Administracyjnego w Warszawie na tę decyzję Prezesa Urzędu Ochrony Danych Osobowych z 21 sierpnia 2020 r. zarzuciła, że decyzja została wydana z naruszeniem art. 7, art. 77 § 1 i art. 80 k.p.a., które mogło mieć istotny wpływ na wynik sprawy. W uzasadnieniu tego zarzutu skarżąca podniosła, że organ nie zgromadził i nie rozpatrzył wyczerpująco materiału dowodowego na okoliczność uznania A G za administratora danych osobowych kandydatów na studia (I i II stopnia oraz jednolitych studiów magisterskich) z lat , obejmujących m. in. imię, nazwisko, nazwisko rodowe, imiona rodziców, numer identyfikacyjny PESEL, płeć, narodowość, obywatelstwo, adres zamieszkania, serię i numer dowodu osobistego bądź innego dokumentu tożsamości, w tym paszportu, numer telefonu komórkowego i/lub

stacjonarnego, informacje o dotychczasowym wykształceniu, informacje o kwalifikacji na studia, zgromadzonych na jego prywatnym komputerze bez wiedzy i zgody skarżącej, cel i sposób przetwarzania tych danych oraz dokonał jego dowolnej oceny i w konsekwencji niezasadnie przyjął, że SGGW ponosi odpowiedzialność za naruszenie przepisów rozporządzenia 2016/679. Zdaniem skarżącej, organ naruszył art. 4 ust. 7 rozporządzenia 2016/679, przyjmując, że Uczelnia była (jest) administratorem tych danych osobowych. Uczelnia stwierdziła, że za administratora tych danych osobowych w rozumieniu art. 4 ust 7 rozporządzenia 2016/679 należało uznać A G w zakresie w jakim bez wiedzy i zgody SGGW zaimportował na swój prywatny komputer zestawy danych osobowych kandydatów na studia oraz określał bez wiedzy i zgody SGGW cel i sposób przetwarzania tych danych. SGGW w Warszawie podniosła, że ze zgromadzonego w toku kontroli materiału dowodowego wynika, że A G w sposób nieuprawniony, bez wiedzy i zgody Uczelni, poza zakresem upoważnienia do przetwarzania danych osobowych oraz z naruszeniem Polityki bezpieczeństwa, określonych w zarządzeniu Rektora SGGW w Warszawie z grudnia 2013r. (nr 88/2013) w sprawie Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych, sukcesywnie przez okres lat poprzedzających kradzież jego komputera przenośnego (listopada 2019 r.) tworzył na twardym dysku komputera, na własne potrzeby i w nie znanej skarżącej celach, bazę danych osobowych kandydatów na studia z tych lat, która – jak wyjaśnił w toku postępowania, zawierać mogła do 100.000 rekordów.

SGGW podała, że z niekwestionowanych okoliczności sprawy wynika, że jako administrator danych osobowych kandydatów na studia gromadzonych w systemie SOK nigdy nie posiadała w jednym czasie takiej ilości rekordów. Uczelnia kierując się zasadą ograniczonego przechowywania danych osobowych (art. 5 ust. 1 lit. e rozporządzenia 2016/679) określiła okres przechowywania danych kandydatów na studia w systemie SOK na 3 miesiące, po czym dane te były trwale usuwane z systemu. Dane kandydatów nieprzyjętych na studia mogły bowiem być w poprzednim stanie prawnym przechowywane zgodnie z prawem jedynie przez okres 12 miesięcy, co wynikało z rozporządzenia Ministra Nauki i Szkolnictwa z dnia 14 września 2011 r. w sprawie dokumentacji przebiegu studiów (Dz. U. Nr 201 z 2011 r., poz. 1188), a następnie przez okres 6 miesięcy zgodnie z rozporządzeniem Ministra Nauki i Szkolnictwa z dnia 16 września 2016 r. w sprawie dokumentacji

przebiegu studiów (Dz. U. z 2016 r., poz. 1554). Na gruncie zaś obecnie obowiązującej ustawy z dnia 28 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668 ze zm.) w związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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), dane te podlegają usunięciu niezwłocznie po tym, gdy przestają być potrzebne, a więc w tym przypadku niezwłocznie po zakończeniu procesu rekrutacji na studia. Uczelnia wywiązywała się z tego obowiązku i usuwała z serwerów obsługujących system SOK bazy zawierające dane osobowe kandydatów na studia w zakreślonym terminie (3 miesiące). W systemie SOK nie było przechowywanych danych kandydatów na studia SGGW jednorazowo w większej ilości niż 20.000.

Skarżąca odwołała się do art. 4 ust 7 rozporządzenia 2016/679, zawierającego definicję administratora danych osobowych i stwierdziła, że Prezes UODO mając dokładną wiedzę o celach i sposobach przetwarzania danych osobowych kandydatów na studia ustalonych przez Uczelnię powinien był poddać analizie cele i sposoby przetwarzania danych przez A G w odniesieniu do zgromadzonych przez niego danych osobowych kandydatów na studia w SGGW z lat r. W świetle ujawnionych w trakcie postępowania kontrolnego okoliczności trudno uznać, że A G realizował tylko i wyłącznie cele i sposoby przetwarzania danych określone przez SGGW skoro Uczelnia każdorazowo po zakończonej rekrutacji (a więc z upływem 3 miesięcy od zasilenia bazy danych systemu SOK rekordami kandydatów) trwale usuwała zgromadzone dane rekrutacyjne z uwagi na wyczerpanie celu przetwarzania. Prezes Urzędu Ochrony Danych Osobowych powinien był w prowadzonym postępowaniu przeprowadzić postępowanie dowodowe w sprawie ustalenia jaki cel i sposób przetwarzania realizował A G skoro przechowywał dane kandydatów na studia na prywatnym komputerze przez okres lat. SGGW nie zgodziła się z zapatrywaniem organu, wyrażonym w zaskarżonej decyzji, że A G pobrane zestawy danych przygotowywał wyłącznie do kwalifikacji poprzez ich odpowiednie filtrowanie w arkuszu kalkulacyjnym według odpowiednich kryteriów kwalifikacyjnych, które są określone dla poszczególnych kierunków studiów, a następnie przedstawiał na spotkaniu kwalifikacyjnym komisji rekrutacyjnej.

Raporty końcowe z zestawieniami statystycznymi według wybranych kryteriów sporządzane były jeszcze w 3 miesięcznym okresie przechowywania danych kandydatów w systemie SOK, a jakiekolwiek porównania statystyczne rok do roku były przygotowywane na potrzeby sprawozdawczości, w tym dla organów kolegialnych Uczelni, bez konieczności przetwarzania tych danych osobowych (w trakcie kontroli wyjaśnienia w tym przedmiocie składał K T). Przechowywane przez A G dane osobowe z rekrutacji zamkniętych (historycznych) nie mogły więc być w żaden sposób ponownie wykorzystane dla jakichkolwiek celów przetwarzania określonych przez Uczelnię i w tym zakresie Prezes UODO winien był dokonać w trakcie postępowania stosownych ustaleń.

Skarżąca podkreśliła, że upoważnienie udzielane corocznie na potrzeby postępowania rekrutacyjnego nie uprawniało A G do zapisywania i przechowywania baz danych osobowych na prywatnym komputerze. Z jego treści nie wynikało również prawo do wynoszenia danych osobowych kandydatów na studia w SGGW poza obszar ich przetwarzania, to jest poza teren SGGW (w chwili kradzieży komputer ten był pozostawiony w samochodzie bez nadzoru jego użytkownika). Z przepisów zarządzenia Rektora SGGW z dnia grudnia 2013 r. w sprawie Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych jednoznacznie wynika, że zapisywanie i przechowywanie jakichkolwiek informacji zawierających dane osobowe może odbywać się wyłącznie na nośnikach służbowych, zapewniających właściwą ochronę poufności i bezpieczeństwa danych osobowych oraz że zabronione jest wynoszenie danych osobowych w postaci wydruków i na nośnikach przenośnych poza obszar przetwarzania bez uzasadnionej przyczyny. Nadto, przywołany akt prawa wewnętrznego SGGW nakazuje odpowiednie zabezpieczenie danych osobowym i wskazuje sposób jego dokonywania stanowiąc, że w celu zabezpieczenia danych przed nieuprawnionym przejęciem, modyfikacją danych na nośnikach i urządzeniach należy korzystać z metody szyfrowania danych, zwłaszcza w przypadku konieczności wynoszenia danych poza chroniony obszar przetwarzania (za zgodą Uczelni). A G znał treść tych regulacji prawnych i stosowne oświadczenie w tym zakresie podpisywał przy okazji każdorazowo udzielanego mu upoważnienia do przetwarzania danych osobowych kandydatów na studia w SGGW w procesie rekrutacji, składał także wymagane

wewnętrznymi procedurami obowiązującymi w SGGW w zakresie ochrony danych osobowych oświadczenie o zapoznaniu się z systemem ochrony danych osobowych zgodnie z przepisami prawa powszechnego oraz wewnętrznego SGGW, a także oświadczenie o zachowaniu danych osobowych w tajemnicy. To wszystko prowadzi do wniosku, że A G miał świadomość ciążącego na nim obowiązku ochrony danych osobowych kandydatów oraz rodzaju, wagi i ilości danych osobowych, które z nieznanych Uczelni przyczyn w sposób nieuprawniony przechowywał na swoim prywatnym komputerze oraz rozmiaru szkody, którą potencjalnie utrata tych danych lub przejęcie ich przez osoby nieuprawnione może wyrządzić osobom, których te dane dotyczą.

Zdaniem skarżącej, konsekwencją niedopuszczalnego i nieuprawnionego przetwarzania przez A G danych osobowych kandydatów na studia w SGGW z lat powinno być uznanie go przez Prezesa UODO w prowadzonym postępowaniu jako administratora tych danych osobowych, które przechowywane były na jego prywatnym komputerze. Zbiór ten bowiem był zbiorem odrębnym od posiadanego przez SGGW w systemie SOK i należało go potraktować jako samodzielną bazę danych osobowych z wszelkimi płynącymi z tego faktu konsekwencjami prawnymi, włącznie z nadaniem przymiotu administratora tej bazy dla A G . Uczelnia, jako administrator własnej bazy danych osobowych w systemie SOK dla danej rekrutacji (przechowywanych przez okres 3 miesięcy) nie miała żadnych możliwości technicznych ani prawnych (był to prywatny komputer) umożliwiających realizację uprawnień administratora wynikających z obowiązujących przepisów wobec zgromadzonych przez A G danych na jego prywatnym komputerze. To zaś prowadzi do wniosku, że zaskarżona decyzja została wydana z naruszeniem art. 4 ust 7 rozporządzenia 2016/679 poprzez jego niezastosowanie wobec pana A G .

W skardze do Sądu Uczelnia zarzuciła ponadto organowi naruszenie art. 5 ust. 1 lit. e rozporządzenia 2016/679 przez nieuzasadnione przyjęcie, że przechowywała sporne dane osobowe przez okres dłuższy niż to było niezbędne do celów, w których te dane były przetwarzane. Skarżąca podkreśliła, że przechowywanie przez A G danych osobowych kandydatów z okresu lat poprzedzających zdarzenie kradzieży jego prywatnego komputera nie oznacza, że administrator nie zastosował się do zasady ograniczonego przechowywania o której mowa w tym przepisie oraz że prawidłowo określiła

właściwy okres przechowywania danych kandydatów na studia (3 miesiące), po którym dane z każdej rekrutacji są trwale usuwane z systemu SOK i co do tego faktu Prezes UODO nie wnosił żadnych zastrzeżeń. Oznacza to, że administrator stosuje się do zasady z art. 5 ust. 1 lit. e rozporządzenia 2016/679.

SGGW zarzuciła że Prezes UODO nieprawidłowo, z naruszeniem art. 5 ust. 1 lit. f rozporządzenia, przyjął, że Uczelnia nie zapewniła odpowiedniego bezpieczeństwa danych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Skarżąca stwierdziła, że przestrzeganie instrukcji wewnętrznych (zarządzenie Rektora Szkoły Głównej Gospodarstwa Wiejskiego z 12.2013 r w sprawie Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych) zapewniało w wystarczającym stopniu spełnienie wymogu bezpieczeństwa i integralności. Skarżąca podkreśliła, że pracownicy Uczelni zgodnie z obowiązującymi procedurami mieli zakaz przetwarzania danych osobowych poza SGGW na jakimkolwiek nośniku (Instrukcja zarządzania systemem informatycznym w ppkt. 7.5 zakazuje wynoszenia danych osobowych w postaci wydruków i na nośnikach przenośnych poza obszar przetwarzania bez uzasadnionej przyczyny). Również w załączniku nr 1 do Polityki bezpieczeństwa, stanowiącym wykaz obszarów, w których przetwarzane są dane osobowe, obszar przetwarzania dla zbioru „Kandydaci na studia" obejmuje wyłącznie siedzibę Uczelni i w przeciwieństwie do innego zbioru (tj. „Studenci"), pozycja ta nie jest opatrzona informacją, że dane mogą być przetwarzane z dowolnego miejsca z uwagi na dostęp do systemu informatycznego przez przeglądarkę internetową.

Zdaniem skarżącej, eksport danych osobowych z SOK na nośnik był dopuszczalny zgodnie z przepisami wewnętrznymi, a nawet konieczny dla celów przetwarzania związanych z rekrutacją, ale ustanowione zakazy zabraniały przetwarzania danych osobowych poza siedzibą SGGW ograniczoną do terenu Uczelni . Nawet gdyby system SOK uniemożliwiał eksport danych na inne komputery lub był ściśle rejestrowany, istniała potencjalna możliwość zdobycia danych z systemu także w inny sposób, np. poprzez wydrukowanie tabel z danymi studentów, zrobienie zdjęć z ekranu z danymi (czego nie można w żaden sposób techniczny ograniczyć). Uzyskane w ten sposób dane studentów mogły następnie, również niezgodnie z ppkt. 7.5 Instrukcji zarządzania systemem informatycznym,

zostać wyniesione poza teren Uczelni gdzie w sposób przypadkowy mogły zostać utracone. Stopień ryzyka naruszenia zasady ograniczenia przechowywania danych (art. 5 ust. 1 lit. e rozporządzenia 2016/679) podczas wykonywania czynności służbowych bądź naruszenia zasady poufności danych (art. 5 ust. 1 lit. f rozporządzenia 2016/679) w wyniku nieprzestrzegania przez pracowników Uczelni procedur wdrożonych w organizacji będzie w każdym z tych przypadków podobny.

W konsekwencji SGGW nie zgodziła się z organem, że proces przetwarzania danych rekrutacyjnych w systemie SOK świadczył o braku kontroli administratora nad tym procesem i dokonywaniu w sposób niewystarczający oceny skuteczności środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych kandydatów na studia. Uczelnia dodała, że celem ograniczenia ryzyka działania czynnika ludzkiego w sposób niezgodny z prawem, zarówno przed dniem kradzieży komputera A G , jak i obecnie, prowadzi stałe szkolenia pracowników Uczelni w zakresie przetwarzania danych osobowych. Zdaniem skarżącej, to nie Uczelnia naruszała art. 5 ust. 1 lit. e oraz art. 5 ust. 1 lit. f rozporządzenia 2016/679 lecz A G w pełni świadomie łamiąc przepisy wewnętrzne w tym zakresie przejmując na siebie funkcję administratora danych osobowych zgromadzonych w nośniku swojego komputera przenośnego (art. 4 ust 7 rozporządzenia 2016/679).

Uczelnia wskazała, że posiada stosowne regulacje wewnętrzne („Politykę Bezpieczeństwa" oraz Instrukcję zarządzania systemem informatycznym), które są aktualizowane w celu dostosowania do przepisów rozporządzenia (w tym m. in. art. 30 ust. 3, art. 33).

Zdaniem skarżącej, zaskarżona decyzja została wydana z naruszeniem art. 5 ust. 2 poprzez nieuwzględnianie w sposób wystarczający, przy korzystaniu z systemu służącego do przetwarzania danych osobowych kandydatów, zasady rozliczalności poprzez pominięcie dowodów z aktów normatywnych obowiązujących w SGGW i innych dowodów z dokumentów i wyjaśnień złożonych w trakcie kontroli prowadzonej przez Prezesa UODO oraz w trakcie postępowania administracyjnego.

Prezes Urzędu Ochrony Danych Osobowych w odpowiedzi na skargę wniósł o jej oddalenie.

Wojewódzki Sąd Administracyjny w Warszawie zważył, co następuje:

Zaskarżona przez Szkołę Główną Gospodarstwa Wiejskiego z siedzibą w Warszawie decyzja Prezesa Urzędu Ochrony Danych Osobowych nie narusza prawa i dlatego jej skarga podlega oddaleniu.

Podstawowy zarzut skargi sprowadza się do nieuznania przez organ A G za administratora danych osobowych i przypisanie naruszeń przepisów rozporządzenia RODO w związku z przetwarzaniem danych kandydatów na studia w SGGW tej Uczelni, a nie A G . Zdaniem skarżącej Uczelni, A G , ze względu na przechowywanie danych osobowych w swoim prywatnym komputerze, bez zgody i wiedzy Uczelni stał się faktycznie odrębnym, samodzielnym administratorem tych danych.

Zarzuty są nieuzasadnione z następujących powodów:

Według art. 4 pkt 7 rozporządzenia RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

W świetle definicji zawartej w rozporządzeniu dla wskazania, kto jest administratorem, kluczowe jest ustalenie, kto decyduje o celu i sposobach przetwarzania danych (kto ustala cele i sposoby przetwarzania danych). Zazwyczaj kompetencje w tym zakresie posiadają podmioty kierujące działalnością danego podmiotu (por. Fajgielski Paweł, Komentarz do art. 4 rozporządzenia nr 2016/679 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), [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, WKP 2018).

Z okoliczności sprawy wynika, że A G w dniu listopada 2019 r., kiedy doszło do kradzieży jego przenośnego prywatnego komputera, nie był podmiotem, który samodzielnie ustalał cele i sposoby przetwarzania danych osobowych kandydatów na studia w SGGW oraz samodzielnie wykonywał czynności przetwarzania, ponieważ był pracownikiem tej Uczelni (w Katedrze

SGGW i pełnił funkcję sekretarza Uczelnianej Komisji Rekrutacyjnej SGGW). Zajmował się przetwarzaniem danych osobowych jako osoba zaangażowana przez Uczelnię w proces przetwarzania danych osobowych, w ramach rekrutacji kandydatów na studia na tej Uczelni. Był zatem niewątpliwie osobą działającą w warunkach zależności (podporządkowania) pracodawcy (SGGW), wynikającej ze stosunku pracy łączącego go z tą Uczelnią.

Należy podkreślić, że z istoty stosunku pracy wynika, że w stosunkach zewnętrznych pracownik nie występuje jako odrębny podmiot prawa (z wyjątkiem, gdy wchodzi w grę jego osobista odpowiedzialność typu karnego czy odpowiedzialność za wykroczenia). Z punktu widzenia prawa jego działania są działaniami pracodawcy i pracodawca ponosi za nie odpowiedzialność, zachowując w stosunku do pracownika regres w postaci możliwości egzekwowania od niego odpowiedzialności odszkodowawczej, porządkowej lub dyscyplinarnej.

Zdaniem Wojewódzkiego Sądu Administracyjnego w Warszawie, nie zmienia tej sytuacji prawnej działanie naruszające czy wykraczające poza zakres powierzonych mu przez pracodawcę zadań i obowiązków pracowniczych (w tym przypadku polegających na przetwarzaniu danych kandydatów na studia). Wówczas dalej mamy do czynienia z działaniem pracownika (naruszającego swoje obowiązki pracownicze), podlegającym jednak zarachowaniu na rzecz pracodawcy, a nie z samodzielnym działaniem osoby, która wykracza w ten sposób poza swój status pracowniczy.

Nie ulega zatem wątpliwości, że w rozpatrywanym przypadku administratorem danych osobowych była SGGW, a nie jej pracownik, A G . W konsekwencji, wbrew zapatrywaniu skarżącej Uczelni, nie ponosi on odpowiedzialności administracyjnej za naruszenie przepisów rozporządzenia RODO.

Przepisy rozporządzenia RODO nakładają na administratora obowiązki w zakresie przestrzegania zasad przetwarzania danych osobowych i obarczają go odpowiedzialnością za ich naruszenie.

Zdaniem Wojewódzkiego Sądu Administracyjnego w Warszawie, Prezes Urzędu Ochrony Danych Osobowych prawidłowo stwierdził, że SGGW w związku z przetwarzaniem danych osobowych kandydatów na studia, naruszył art. 5 ust. 1 lit. e, art. 5 ust. 1 lit f, art. 5 ust. 2, art. 24 ust. 1, art. 25 ust 1, art. 32 ust. 1 lit b, art. 32

ust. 1 lit. d, art. 32 ust. 2 i art. 38 ust. 1, art. 39 ust. 1 lit b i art. 39 ust. 2 rozporządzenia 2016/679.

W myśl zasady ograniczenia przechowywania danych osobowych, o której mowa w art. 5 ust. 1 lit. e rozporządzenia, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne). Zgodnie z zasadą integralności i poufności przetwarzania danych osobowych (art. 5 ust. 1 lit. f rozporządzenia), dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Art. 5 ust. 2 rozporządzenia stanowi, że administrator jest odpowiedzialny za przestrzeganie podstawowych zasad dotyczących przestrzegania określonych w ust.1 tego artykułu i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Trzeba podkreślić, że z tego przepisu wynika domniemanie odpowiedzialności administratora za naruszenie tych zasad, jako że na nim spoczywa ciężar wykazania ich przestrzegania.

Administrator danych powinien zatem przeprowadzić analizę ryzyka i ocenić, z jakimi zagrożeniami ma do czynienia. Stosownie do art. 24 ust. 1 i art. 25 ust. 1 rozporządzenia, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, powinien wdrożyć odpowiednie środki techniczne i organizacyjne, pozwalające skutecznie zabezpieczyć przetwarzane dane, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby, a w razie sporu z osobą, której dane dotyczą, albo z organem nadzorczym, móc przedstawić dowody na to, że przestrzega tych zasad i przepisów. Według art. 32 ust. 1 rozporządzenia RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień

bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (pkt b) oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (pkt d). Przepis ust. 2 art. 32 powołanego rozporządzenia stanowi, że oceniając czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Administrator danych osobowych jest odpowiedzialny także za to, aby inspektor ochrony danych monitorował przestrzeganie przepisów dotyczących przetwarzania danych osobowych oraz polityki administratora w dziedzinie ochrony danych osobowych, przeprowadzał szkolenia personelu uczestniczącego w operacjach przetwarzania oraz audyty, uwzględniając ryzyko związane z operacjami przetwarzania (art. 39 ust. 1 lit. b i art. 39 ust. 2 rozporządzenia 2016/679) oraz był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1 rozporządzenia).

Z obszernego materiału dowodowego bardzo szeroko zaprezentowanego w uzasadnieniu zaskarżonej decyzji wynika zdaniem Sądu, że skarżąca Uczelnia dopuściła się naruszenia tych zasad, starając się przerzucić odpowiedzialność za te naruszenia na swojego pracownika, pomijając swój udział w powstaniu naruszeń, polegający zarówno na niedopełnieniu swoich obowiązków pracodawcy w zakresie kontroli pracy pracownika, jak i niedopełnieniu obowiązków administratora danych osobowych, określonych w rozporządzeniu RODO.

Wojewódzki Sąd Administracyjny w Warszawie podziela zapatrywanie organu, że Uczelnia jako administrator danych osobowych kandydatów na studia w sposób niewystarczający dokonywała oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania tych danych i w ten sposób naruszyła art. 5 ust. 1 lit. e, art, 5 ust. 1 lit. f, art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d, art. 32 ust. 2 i art. 38 ust. 1 oraz art. 5 ust. 2 rozporządzenia 2016/679. .

Uczelnia ograniczyła się do odebrania od A G oświadczenia o zachowaniu danych osobowych w tajemnicy i o zapoznaniu się z

zasadami przetwarzania danych osobowych. Mając świadomość istnienia technicznej możliwości przetwarzania polegającej na eksportowaniu na zewnętrzny nośnik danych osobowych z systemu SOK, nie kontrolowała jednak w sposób dostateczny procesu przetwarzania przez niego danych osobowych w związku z czynnościami podejmowanymi, nie weryfikowała prawidłowości przetwarzania przez pracownika tych danych. Świadczy o tym to, że nie posiadała wiedzy o możliwości pobierania danych z SOK bez rejestrowania tego procesu w systemie informatycznym oraz o tym, że jej pracownik A G , z SOK importował na swój prywatny komputer zestawy danych osobowych kandydatów na studia z okresu ostatnich lat, a więc przetwarzał je poza przewidziany okres 3 miesięcy, poza zakresem upoważnienia oraz gromadził poza obszarem przetwarzania (upoważnienie nie obejmowało zapisywania i przechowywania danych osobowych na prywatnym komputerze i wynoszeniu ich poza teren SGGW).

Z okoliczności sprawy wynika, że skarżąca Uczelnia nie dokonała oceny ryzyka w zakresie możliwości naruszenia zasady poufności danych osobowych czy zasady ograniczenia przechowywania danych (art. 5 ust. 1 lit f i lit e rozporządzenia), wynikającego z zagrożenia jakim jest możliwość eksportowania z systemu SOK danych osobowych kandydatów na studia w SGGW na nośnik zewnętrzny. SGGW nie wykazała, zgodnie z zasadą rozliczalności, aby administrator danych osobowych dokonał analizy ryzyka związanego z przetwarzaniem danych osobowych kandydatów na studia w SGGW oraz nadzorował przestrzeganie przez A G zasad dotyczących przetwarzania danych osobowych, określonych w przepisach prawa powszechnie obowiązującego oraz w Polityce Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych. Inspektor danych osobowych nie był angażowany w proces rekrutacji na studia, nie był włączany przez administratora w sprawy dotyczące ochrony danych osobowych w zakresie podejmowanych rozwiązań technicznych w ramach funkcjonowania SOK (art. 38 ust. 1), a wykonując swoje zadania nie uwzględnił ryzyka związanego z operacjami przetwarzania danych, co stanowi o naruszeniu przez Uczelnię, jako administratora danych, art. 24 ust. 1, art. 32 ust. 1, art. 32 ust. 2, art. 38 ust. 1, art. 39 ust. 1 lit b i ary. 39 ust. 2 rozporządzenia 2016/679.

Można dodać, że A G mimo że był zaangażowany w proces przetwarzania danych osobowych na Uczelni podczas rekrutacji

kandydatów na studia, nie uczestniczył w szkoleniu dotyczącym ochrony danych osobowych w procesie przetwarzania.

Z treści art. 84 ust. 1 pkt b rozporządzenia RODO wynika, że przewidziana w rozporządzeniu odpowiedzialność administracyjna w postaci kar pieniężnych jest odpowiedzialnością obiektywną (za sam skutek czyli naruszenie prawa), a więc niezależną od winy sprawcy (wina może mieć jedynie wpływ na wysokość kary).

Z tych względów prawnych wyjaśnienia Uczelni, że ze swej strony dokładała starań w zakresie przestrzegania zasad przetwarzania danych osobowych kandydatów na studia nie mogły mieć istotnego znaczenia przy podjęciu decyzji o nałożeniu kary. .

Zdaniem Sądu, Prezes Urzędu Ochrony Danych Osobowych ustalając wysokość kary za nieprawidłowe przetwarzanie danych osobowych, uwzględnił okoliczności wymienione w art. 83 ust. 2 rozporządzenia, takie jak: charakter, wagę i czas trwania naruszenia (lat), kategorie danych osobowych, których dotyczyło naruszenie; liczbę poszkodowanych osób (100 000), rozmiar poniesionej przez nie szkody; wysoki stopień odpowiedzialności administratora, który w procesie przetwarzania danych nie stosował podstawowych zasad dotyczących przetwarzania danych osobowych, określonych w rozporządzeniu, ale także okoliczności łagodzące, mające wpływ na wymiar kary, takie jak podjęcie przez Uczelnię możliwych działań mających na celu usuniecie naruszenia, dobrą współpracę Uczelni z organem nadzorczym w trakcie postępowania, w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków; fakt, że Uczelnia nie dopuściła się uprzednio naruszenia przepisów rozporządzenia.

Z tych wszystkich względów Wojewódzki Sąd Administracyjny w Warszawie stwierdził, ze zarzuty skargi są nieuzasadnione i dlatego na podstawie art. 151 ustawy z 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2019 r., poz. 2325 ze zm.), orzekł jak w sentencji.

WOJEWÓDZKI SĄD ADMINISTRACYJNY W WARSZAWIE