GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 18 września 2014 r.

DIS/DEC-916/14/72987

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 26 ust. 1 pkt 1 i 4, art. 31 ust. 1 i 2, art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182), § 7 ust. 1 pkt 1, 2 i 3, § 7 ust. 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz częścią A pkt III ppkt 1 i częścią B pkt VIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez W.,

I. Nakazuję W. usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. **Zaprzestanie udostępniania A. danych osobowych […] W., którym przyznane zostały miejsca w […] oraz w […], położonych na terenie […], bez podstawy prawnej, tj. bez zawarcia z ww. […] umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182), określającej cel i zakres, w jakim A. może przetwarzać powierzone jej dane osobowe, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Zmodyfikowanie systemu informatycznego o nazwie „[…]" (wykorzystywanego do przetwarzania danych osobowych […] W. zakwaterowanych w […]), w taki sposób, aby zapewniał dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu,**

ul. Stawki 2
00-193 Warszawa

tel. 860-70-81
fax 860-70-90
www.giodo.gov.pl

identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz źródła danych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. **Zmodyfikowanie systemu informatycznego o nazwie „[…]" (wykorzystywanego do przetwarzania danych osobowych […] W. zakwaterowanych w […]), w taki sposób, aby zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zapewnienie, aby hasło wykorzystywane przez Panią […], samodzielnego referenta, w procesie uwierzytelnienia użytkownika w systemie operacyjnym komputera używanego do przetwarzania danych osobowych […] W. zawierało cyfry lub znaki specjalne, od dnia, w którym niniejsza decyzja stanie się ostateczna.**

II. W pozostałym zakresie postępowanie umarzam.

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w W., zwanym dalej „W.", w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt […]), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182), zwaną dalej „ustawą", oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanym dalej „rozporządzeniem". Zakresem kontroli objęto przetwarzanie danych osobowych przez W. w związku z funkcjonowaniem […] W., w szczególności z ubieganiem się o miejsca w […], rozdziałem miejsc, zakwaterowaniem i wykwaterowaniem mieszkańców, odwiedzinami u mieszkańców. W toku kontroli odebrano od pracowników W. ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Rektora W.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych W., jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Nieusuwaniu ze skrzynek poczty elektronicznej pracowników W. list zawierających dane osobowe […] W., przekazywanych pocztą uczelnianą pomiędzy […] a […] (art. 26 ust. 1 pkt 4 ustawy).
2. Udostępnianiu bez podstawy prawnej A. danych osobowych […] W., w związku z brakiem umowy powierzenia przetwarzania danych osobowych zawartej z ww. […] (art. 26 ust. 1 pkt, ustawy i art. 31 ust. 1 i 2 ustawy).
3. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi zbioru danych dotyczącego osób, którym zostały wystawione faktury VAT za zakwaterowanie w […] (art. 40 ustawy).
4. Niezapewnianiu przez system informatyczny o nazwie „[…]", służący do przetwarzania danych osobowych […] zakwaterowanych w […], odnotowania daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz źródła danych (§ 7 ust. 1 pkt 1, 2 i 3 rozporządzenia).
5. Niezapewnianiu przez system informatyczny o nazwie „[…]", służący do przetwarzania danych osobowych […] zakwaterowanych w […], sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. 3 rozporządzenia).
6. Braku programu antywirusowego na komputerze użytkowanym przez Panią […], samodzielnego referenta, używanym do przetwarzania danych osobowych […] W. (część A pkt III ppkt 1 załącznika do rozporządzenia).
7. Wykorzystywaniu podczas logowania do systemu operacyjnego na komputerze użytkowanym przez Panią […], samodzielnego referenta, używanym do przetwarzania danych osobowych […] W., hasła składającego się z 5 znaków i zawierającego małe litery (częścią B pkt VIII załącznika do rozporządzenia).

W związku z powyższym, w dniu […] sierpnia 2014 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma […]).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego p.o. Kanclerza W. pismem z dnia […] sierpnia 2014 r., nr […], złożył wyjaśnienia, w których poinformował, że:

1. Listy zawierające dane osobowe […] W. przekazywane pocztą uczelnianą pomiędzy […] a […] będą usuwane ze skrzynek poczty elektronicznej pracowników W. niezwłocznie po potwierdzeniu otrzymania tych danych przez adresata. Takie rozwiązanie zostało zapisane

w znowelizowanej „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, stanowiącej załącznik do zarządzenia Rektora W. nr […] z dnia […] grudnia 2007 r.

2. Powierzenie przetwarzania danych osobowych A. zostanie uregulowane aneksem do umowy nr […] z dnia […] czerwca 2014 r.
3. Zbiór danych dotyczący osób, którym zostały wystawione faktury VAT za zakwaterowanie w […] został zgłoszony do rejestracji Generalnemu Inspektorowi.
4. W systemie informatycznym o nazwie „[…]” pracownicy […] W. podjęli działania mające na celu uzyskanie kodów źródłowych oraz identyfikację rodzaju gromadzonych przez ten system danych w strukturze bazy danych. Do dnia […] września 2014 r. planowane jest uzupełnienie systemu „[…]” o moduł audytu wprowadzania i zmian danych osobowych oraz o moduł raportowania, który umożliwi sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie m.in. datę pierwszego wprowadzenia danych do systemu, identyfikator użytkownika wprowadzającego dane osobowe do systemu oraz źródło danych.
5. Na komputerze Pani […] zainstalowano program antywirusowy oraz dostosowano hasło do wymaganych 8 znaków składających się z małych i wielkich liter.

Ponadto, do pisma z dnia […] sierpnia 2014 r., nr […], zostały załączone dowody mające potwierdzić usunięcie uchybień stwierdzonych w toku kontroli.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 26 ust. 1 pkt 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem. W myśl art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Natomiast stosownie do art. 31 ust. 2 ustawy, podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

Przeprowadzona kontrola wykazała, że dane osobowe […] W., którym przyznane zostały miejsca w […] oraz w […], położonych na terenie […], są przekazywane przez W. do tych […]. Jednocześnie ustalono, że podmiotem uprawnionym do rezerwowania pokoi mieszkalnych w […] położonych na terenie […] jest A., z którą W. podpisał w dniu […] czerwca 2013 r. umowę nr […]. W związku z tym, że przekazanie danych do ww. […] jest równoznaczne z powierzeniem A. przetwarzania tych danych, to w umowie powinny zostać zawarte postanowienia określające cel i zakres, w jakim A. może przetwarzać dane osobowe. Tymczasem w umowie nr […] z dnia […]

czerwca 2013 r. takich postanowień nie zawarto, co oznacza, że umowa ta nie może zostać uznana za umowę powierzenia przetwarzania danych osobowych.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego p.o. Kanclerza W. poinformował, że powierzenie przetwarzania danych osobowych A. zostanie uregulowane aneksem do umowy nr […] z dnia […] czerwca 2014 r. Podjęcie tych działań nie może jednak stanowić podstawy do uznania, że w tym zakresie został przywrócony stan zgodny z prawem. Nadal bowiem W. nie ma zawartej z A. umowy powierzenia przetwarzania danych osobowych. W konsekwencji należy stwierdzić, że W. nie dołożył szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności nie zapewnił, aby dane te były przetwarzane zgodnie z prawem.

Zgodnie z § 7 ust. 1 pkt 1, 2 i 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada jedna osoba oraz źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą. W myśl § 7 ust. 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.

W toku kontroli ustalono, że pracownicy W. nie dysponują informacjami, czy system informatyczny o nazwie „[…]", służący do przetwarzania danych osobowych […] zakwaterowanych w […], zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz źródła danych. Ponadto ustalono, że system „[…]" nie posiada funkcjonalności umożliwiającej uzyskanie informacji o dacie wprowadzenia danych […] do systemu oraz identyfikatorze użytkownika wprowadzającego dane, a także nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego p.o. Kanclerza W. poinformował, że pracownicy […] W. podjęli działania mające na celu uzyskanie kodów źródłowych systemu informatycznego o nazwie „[…]" oraz identyfikację rodzaju gromadzonych przez ten system danych w strukturze bazy danych. Ponadto wskazał, że do dnia […] września 2014 r. planowane jest uzupełnienie systemu „[…]" o moduł audytu wprowadzania i zmian danych osobowych oraz o moduł raportowania, który umożliwi sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie m.in. datę pierwszego

wprowadzenia danych do systemu, identyfikator użytkownika wprowadzającego dane osobowe do systemu oraz źródło danych.

Należy uznać, że podjęcie tych działań nie może jednak stanowić podstawy do uznania, że w tym zakresie został przywrócony stan zgodny z prawem. Wykorzystywany w W. system „[…]" nadal bowiem nie spełnia wymogów określonych w § 7 ust. 1 pkt 1, 2 i 3 oraz § 7 ust. 3 rozporządzenia i w związku z tym Generalny Inspektor nakazał w tym zakresie przywrócenie stanu zgodnego z prawem wyznaczając 30-dniowy termin wykonania decyzji.

Zgodnie z częścią B pkt VIII załącznika do rozporządzenia, w przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

W toku kontroli ustalono, że podczas logowania do systemu operacyjnego na komputerze użytkowanym przez Panią […], samodzielnego referenta, wymagane jest podanie identyfikatora i hasła składającego się z 5 znaków. Hasło zawiera małe litery.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego p.o. Kanclerza W. poinformował, że wykorzystywane przez Panią […] hasło zostało dostosowane do wymaganych 8 znaków składających się z małych i wielkich liter. W związku z powyższym wyjaśnieniem należy wskazać, że zgodnie z powołanym wyżej przepisem załącznika do rozporządzenia hasło powinno zawierać, oprócz małych i wielkich liter, również cyfry lub znaki specjalne. Tymczasem w stosowanym przez Panią […] haśle brak jest cyfr i znaków specjalnych, co oznacza, że nie spełnia ono wymogów określonych w części B pkt VIII załącznika do rozporządzenia.

Jednocześnie, na podstawie złożonych przez p.o. Kanclerza W. pisemnych wyjaśnień oraz przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. Określony został okres przechowywania na skrzynkach poczty elektronicznej pracowników W. listy zawierających dane osobowe […] W.
2. Zbiór danych dotyczący osób, którym zostały wystawione faktury VAT za zakwaterowanie w […], został zgłoszony do rejestracji Generalnemu Inspektorowi.
3. Na komputerze Pani […], samodzielnego referenta, zainstalowano program antywirusowy.
4. Hasło wykorzystywane przez Panią […], samodzielnego referenta, w procesie uwierzytelnienia użytkownika składa się z 8 znaków i zawiera małe oraz wielkie litery.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe w całości albo w części, organ administracji

publicznej wydaje decyzję o umorzeniu postępowania odpowiednio w całości albo w części. Przesłanką umorzenia postępowania, na podstawie art. 105 § 1 k.p.a., jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny", czyli z każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z dnia 21 stycznia 1999 r., SA/Sz1029/97).

W toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego w tym zakresie należało je umorzyć.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji.

W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2012 r., poz. 1015 z późn. zm.).