GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak - Jomaa

Warszawa, dnia 13 listopada 2015 r.

DIS/DEC/884/15/98497
dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 oraz 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. 23 ust. 1 pkt 1 w zw. z art. 36 ust. 2, art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.), § 4 pkt 4 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 IV ust. 2 załącznika do ww. rozporządzenia w sprawie przetwarzania danych osobowych przez S. Sp. z o. o.,

I. Nakazuję S. Sp. z o. o. przywrócenie stanu zgodnego z prawem poprzez:

1. Nadanie osobom dopuszczonym do przetwarzania danych osobowych upoważnień, w terminie 30 dnia od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Uzupełnienie dokumentacji stanowiącej politykę bezpieczeństwa w zakresie opisu przepływu danych pomiędzy systemami, z uwzględnieniem systemu o nazwie A., w którym przetwarzane są dane osobowe pracowników i kandydatów do pracy w Spółce, w terminie 30 dnia od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie umarzam postępowanie.

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w S. Sp. z o. o. (dalej: Spółka), kontrolę 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 z późn. zm.), 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 przez S. danych osobowych pracowników, w tym w szczególności pozyskiwanie danych osobowych o narodowości pracowników.

W toku kontroli odebrano ustne wyjaśnienia od pracowników Spółki oraz skontrolowano systemy informatyczne służące do przetwarzania danych osobowych. Stan faktyczny szczegółowo opisano w protokole kontroli, który został podpisany przez Członka Zarządu zagranicznego przedsiębiorcy oraz osobę uprawnioną do reprezentowania.

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

1. Dopuszczeniu do przetwarzania danych osobowych w Spółce osób, którym nadano upoważnienia niezgodnie z art. 37 ustawy.
2. Nieuwzględnieniu w prowadzonej w Spółce dokumentacji stanowiącej politykę bezpieczeństwa opisu przepływu danych pomiędzy systemami z uwzględnieniem systemu informatycznego o nazwie A, w którym przetwarzane są dane osobowe pracowników i kandydatów do pracy w Spółce (art. 36 ust. 2 w zw. z § 4 pkt 4 rozporządzenia).
3. Niedopełnieniu obowiązku, aby w systemach sieciowych oraz w systemie informatycznym o nazwie A (w którym przetwarzane są dane osobowe pracowników i kandydatów do pracy w Spółce) hasła używane do uwierzytelniania użytkowników były zmieniane nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).

W związku z powyższym, w dniu […] września 2015 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. […]).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego osoba reprezentująca zagranicznego przedsiębiorcę w Oddziale pismem z dnia […] września 2015 r. złożyła wyjaśnienia, z których wynika, że:

1. W Spółce nadane zostaną pracownikom nowe imienne upoważnienia do przetwarzania danych osobowych.
2. Dokumentacja opisująca przetwarzanie danych osobowy w Spółce zostanie dostosowana do wymogów ustawy o ochronie danych osobowych i rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
3. W Spółce zastosowane zostały środki techniczne i organizacyjne służących zabezpieczaniu danych osobowych przetwarzanych w systemach informatycznych, w tym również w zakresie zarządzania tożsamością użytkowników i dostępem do systemu A. Są to środki zapewniające wystarczający i odpowiedni do zagrożeń poziom zabezpieczenia danych (pomimo iż hasła dostępu do systemu A co do zasady zmieniane są co 90 dni). Zastosowane przez Spółkę środki to między innymi: polityka jakości i złożoności haseł tzw. […]; stosowanie dodatkowo haseł użytkowników (które podlegają tym samym rygorom co […]); wprowadzenie Programu ochrony przed utratą danych […]; formy kontroli dostępu do systemu A […]; funkcjonowanie w Spółce specjalnego programu zarządzania usługami zabezpieczenia polegającymi na monitorowaniu bezpieczeństwa sieci i zapewnieniu zdolności do reagowania na zagrożenia oraz monitorowaniu systemu i użytkowników w celu identyfikacji nieprawidłowych działań.

Ponadto, Spółka powołała się na decyzje Generalnego Inspektora (DESIWM/DEC-406/18293/09, DESiWM/DEC-440/19191/09) w których pomimo braku wymogu zmiany haseł nie rzadziej niż co 30 dni, przy zastosowaniu innych środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych uznano, że został zapewniony wystarczający poziom ochrony danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu analizy całokształtu materiału dowodowego zebranego w niniejszej sprawie zważył, co następuje:

1. Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Jak ustalono, pracownicy Spółki zostali zbiorczo upoważnieni do przetwarzania danych osobowych w Spółce w zakresie powierzonych obowiązków. Osoby wymienione w dokumencie o nazwie […] otrzymały zgodę na przetwarzanie danych osobowych w Spółce. Zgoda została wyrażona poprzez podpisanie ww. dokumentu przez administratora bezpieczeństwa informacji, który jednak nie posiada pisemnego upoważnienia do nadawania upoważnień do przetwarzania danych osobowych w imieniu administratora danych.

W swoich wyjaśnieniach Spółka wskazała, że trwają prace nad wdrożeniem nowych imiennych upoważnień do przetwarzania danych osobowych, które będą nadawane pracownikom.

Biorąc pod uwagę powyższe, należy uznać, iż w Spółce w dalszym ciągu osobom dopuszczonym do przetwarzania danych osobowych nie nadano upoważnień spełniających wymogi określone w powołanym wyżej przepisie. Samo podjęcie działań nie może stanowić podstawy do uznania, że został przywrócony stan zgodności z prawem.

2. Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Dokumentacja, o której jest mowa wyżej, zgodnie z ust. 3, powinna zostać wdrożona przez administratora danych. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności sposób przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia).

Jak ustalono w toku kontroli w Spółce został wdrożony dokument o nazwie […], który jest traktowany jako „Polityka Bezpieczeństwa". Ponieważ Spółka jest oddziałem St. w Spółce obowiązują również dokumenty wewnętrzne opracowane w języku angielskim przez St. Dokumenty te szczegółowo regulują kwestie bezpieczeństwa i zarządzania systemami informatycznymi S. (opisują kwestie jakie powinna zawierać instrukcja zarządzania systemem informatycznym). Po analizie przedstawionych przez Spółkę dokumentów stwierdzono, że nie zawierają one opisu przepływu danych pomiędzy systemami, w tym uwzględniającego system informatyczny o nazwie A, w którym przetwarzane są dane osobowe pracowników i kandydatów do pracy w Spółce.

W swoich wyjaśnieniach Spółka wskazała, że dokumentacja opisująca przetwarzanie danych osobowych w Spółce zostanie dostosowana do wymogów ustawy o ochronie danych osobowych i rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Z uwagi na to, ze Spółka nie przedstawiła dowodów potwierdzających opracowanie i wdrożenie dokumentacji uzupełnionej w zakresie opisu przepływu danych pomiędzy systemami nie można uznać, że we wskazanym zakresie został przywrócony stan zgodny z prawem.

Jednocześnie na podstawie przedstawionych dowodów należy uznać, że pozostałe uchybienie stanowiące przedmiot postępowania administracyjnego, zostało usunięte, tj. zastosowane przez Spółkę środki techniczne i organizacyjne służące zabezpieczaniu danych osobowych przetwarzanych w systemach informatycznych, w tym również w zakresie zarządzania tożsamością użytkowników i dostępem do systemu A (w tym polityka złożoności haseł […] itd.),

pozwalają na stwierdzenie, iż pomimo zmiany haseł rzadziej niż co 30 dni, zapewniają one ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

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 materialnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. S.A./Sz1029/97).

Z uwagi zatem na to, że pozostałe uchybienie stwierdzone w toku kontroli zostało uznane za usunięte, postępowanie w tym zakresie należało 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.

Jednocześnie informuję, iż 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 2014 r., poz. 1619).