GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak - Jomaa

Warszawa, dnia 26 maja 2015 r.

DIS/DEC-441/15/41273
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 pkt 6 oraz art. 22 w związku z art. 26 ust. 1 pkt 3, art. 31 ust. 1, art. 36 ust. 1 i ust. 2, art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.) oraz § 4 pkt 2 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez P. S.A. (dalej: Spółka),

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

1. Zaprzestanie przetwarzania numerów PESEL w celu ewidencji osób wchodzących do budynków Spółki oraz z nich wychodzących, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Usunięcie numerów PESEL pozyskanych w celu ewidencji osób wchodzących do budynków Spółki oraz z nich wychodzących, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Opracowanie procedur określających termin przechowywania (w tym usuwania) danych osobowych przetwarzanych w systemie informatycznym o nazwie „A” (w którym przetwarzane są dane osób wchodzących do budynków Spółki), w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę (sygn. […]) w Spółce w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182, ze 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 przetwarzane przez Spółkę danych osobowych z wyłączeniem danych osobowych pracowników oraz kandydatów do pracy. Stan faktyczny szczegółowo opisano w protokole kontroli, który został podpisany przez Członków Zarządu Spółki.

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

1) przetwarzaniu nr PESEL w celu ewidencji osób wchodzących do budynków Spółki oraz z nich wychodzących (art. 26 ust. 1 pkt 3 ustawy),

2) niezawarciu z E. Sp. z o. o. oraz S. Sp. z o.o. pisemnej umowy powierzenia przetwarzania danych osobowych przetwarzanych w systemie monitoringu wizyjnego (art. 31 ust. 1 ustawy),

3) niezawarciu z E Sp. z o. o. oraz ED Sp. z o.o. pisemnej umowy powierzenia przetwarzania danych osobowych przetwarzanych w systemie informatycznym o nazwie A (art. 31 ust. 1 ustawy),

4) nieopracowaniu procedur określających termin przechowywania (w tym usuwania) danych osobowych (wizerunek) rejestrowanych za pomocą urządzenia technicznego służącego do zapisu obrazu oraz przetwarzanych w systemie informatycznym o nazwie „A” (art. 36 ust. 1 ustawy),

5) niewskazaniu w prowadzonym przez Spółkę wykazie zbiorów danych osobowych, na który składa się dokument o nazwie „Wykaz zasobów danych osobowych i systemów ich przetwarzania” programów zastosowanych do przetwarzania tych danych (§ 4 pkt 2 rozporządzenia),

6) niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych, w którym przetwarzane są dane osób trzecich zarejestrowanych za pomocą urządzenia służącego do rejestracji obrazu (art. 40 ustawy).

W piśmie z dnia […] kwietnia 2015 r. (sygn. […]), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Spółka została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, Członkowie Zarządu Spółki pismem z dnia […] kwietnia 2015 r. (znak […]) złożyli wyjaśnienia, w których poinformowali, iż:

1) w celu realizacji celów Spółki, tj. niezakłóconej produkcji energii elektrycznej i cieplnej, właściciel – […] uznał zakłady Spółki za obiekty podlegające obowiązkowej ochronie. Jeden ze składników mienia Spółki jest objęty […]. Ponadto, Spółka uzyskała […]. Nakłada to na Spółkę obowiązek zapewnienia właściwego poziomu ochrony fizycznej i technicznej obiektom produkcyjnym, poziom ten wymaga uzgodnień i akceptacji ze strony […] i opisany jest w Planie Ochrony dostosowanym do zagrożeń każdego zakładu Spółki. Plany te zobowiązują Spółkę m.in. do zapewnienia ewidencji osób wchodzących i wychodzących w celu minimalizacji ryzyka ze strony osób przebywających na terenie Spółki np. kradzieży, sabotażu, aktów wandalizmu lub terroru. Obecnie na terenie zakładów np. […] przebywa dziennie setki, czasem tysiące osób, z czego 2/3 to pracownicy licznych firm obcych. W ostatnich latach na terenie Spółki miały miejsce dziesiątki przypadków, gdy zostały usunięte osoby stanowiące zagrożenie dla współpracowników lub infrastruktury Spółki. W wielu przypadkach zagrożenie było na tyle poważne, że Spółka chce i musi mieć pewność niedopuszczenia do ponownego wstępu w przyszłości takich osób (np. w 2007 r. zgłoszenie przez pracownika firmy zewnętrznej podłożenia ładunku wybuchowego na terenie zakładu, co skutkowało ewakuacją zakładu i ogromnymi stratami finansowymi). W obecnie obserwowanej sytuacji na rynku pracy firm świadczących usługi w naszych zakładach, tj. wysokiej rotacji pracowników, elastyczności form zatrudnienia, jednoczesnej pracy w kilku firmach Spółka nie ma żadnej możliwości kontroli faktycznego celu uzyskania uprawnień dostępowych przez osoby z zewnątrz. Niedoskonałość weryfikacji i ewidencji osób firm zewnętrznych zwielokrotnia fakt dużej powtarzalności polskich imion i nazwisk. Obecnie w systemie informatycznym Spółki są dziesiątki osób o tych samych imionach i nazwiskach. W opisanych powyżej okolicznościach jedynie nr PESEL pozwala Spółce na wcześniejszą, jednoznaczną weryfikację osoby niepożądanej. W przeszłości miało miejsce wiele przypadków, gdzie nr PESEL pozwolił Spółce ujawnić osobę niepożądaną ponownie starającą się przeniknąć na nasz teren np., jako pracownik innej firmy. Zmuszenie Spółki do pozbycia się tego narzędzia spowoduje obniżenie poziomu bezpieczeństwa zakładów Spółki - także elementów

Infrastruktury Krytycznej, i bezpieczeństwa informacji niejawnych, co Spółka musiałaby zgłosić organom kontrolującym bezpieczeństwo,

2) zostały podpisane umowy powierzenia przetwarzania danych osobowych z ED. Sp. z o. o. oraz E. Sp. z o. o. (kopia umowy powierzenia przetwarzania danych osobowych zawartej w dniu […] kwietnia 2015 r. z E. Sp. z o. o. oraz kopia umowy powierzenia przetwarzania danych osobowych zawartej w dniu […] kwietnia 2015 r. z ED. Sp. z o. o. stanowią załącznik do niniejszego pisma). Jednocześnie wskazano, iż umowa powierzenia przetwarzania danych osobowych z S. Sp. z o. o., znajduje się obecnie w podpisie. Po podpisaniu, kopia umowy zostanie dostarczona do Biura GIODO,

3) została opracowana i wdrożona „Procedura przechowywania zarejestrowanych obrazów w systemach telewizji dozorowej" (kopia ww. procedury stanowi załącznik do niniejszego pisma).

4) został opracowany projekt dokumentu o nazwie „Procedura archiwizacji oraz usuwania danych w […]" określającej terminy przechowywania oraz usuwania danych. Jednak wdrożenie procedury wymaga przebudowy systemu informatycznego o nazwie „A". Producent oprogramowania zadeklarował wykonanie niezbędnych zmian w oprogramowaniu w okresie trzech miesięcy od momentu otrzymania zlecenia. Aby Spółka mogła zlecić wykonanie tych prac, niezbędna jest decyzja Generalnego Inspektora Ochrony Danych Osobowych w zakresie przetwarzania przez Spółkę nr PESEL,

5) podjęte zostały działania korygujące mające na celu usunięcie uchybienia i powiązania ze sobą zbiorów danych osobowych z systemami ich przetwarzania (aktualny „Wykaz zbiorów danych osobowych i systemów ich przetwarzania" stanowi załącznik do niniejszego pisma),

6) zgłoszono do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „B" (zgłoszenie nr R: […]).

Ponadto Członkowie Zarządu Spółki pismem z dnia […] maja 2015 r. (znak […]) przesłali kopię umowy powierzenia przetwarzania danych osobowych przetwarzanych w systemie monitoringu wizyjnego zawartej w dniu […] kwietnia 2015 r. z S. Sp. z o.o.

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 3 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; merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

W toku kontroli ustalono, iż zgodnie z dokumentem o nazwie „Instrukcja kontroli ruchu osobowego i materiałowego” w Spółce uregulowano tryb wydawania oraz ewidencjonowania przepustek – identyfikatorów.

Ja ustalono system przepustkowy ma na celu identyfikację i ewidencję osób przebywających na terenie Spółki, uniemożliwienie przedostania się na teren osób nieuprawnionych oraz uniemożliwienie nieformalnego wynoszenia i wywożenia składników majątkowych Spółki. Powołany wyżej dokument nie uwzględnia skanowania dokumentów, za pomocą czytnika […], które ma miejsce na portierni siedziby Spółki oraz na portierni […] od początku bieżącego roku. Skaner dokumentów umożliwia skanowanie dwóch typów dokumentów, tj. prawa jazdy oraz dowodu osobistego. Skanowanie odbywa się w dwóch etapach. Etap pierwszy określa rodzaj dokumentu poprzez ustalenie ogólnego układu graficznego i nie zachowuje tego rozkładu w pamięci. W drugim etapie skanowane są tylko wybrane obszary dokumentu, w którym znajdują się odpowiednio: imię, nazwisko, numer PESEL, nr prawa jazdy oraz seria i nr dowodu osobistego. Ww. dane osobowe przetwarzane są w systemie informatycznym o nazwie A. Spółka nie przetwarza skanów dokumentów tylko ww. dane. Ponadto do ww. systemu wprowadzana jest ręcznie dana dotycząca miejsca zatrudnienia osoby wchodzącej na teren Spółki (jeżeli wchodzi na teren Spółki w celach zawodowych) bądź informacja, iż jest to osoba prywatna. Przedmiotowe dane są przetwarzane w celu rejestracji wejść i wyjść oraz w celu przebywania w obiektach Spółki.

Podstawą prawną przetwarzania przez Spółkę danych osobowych w systemie informatycznym o nazwie A jest art. 23 ust. 1 pkt 5 ustawy, tj. przetwarzanie ww. danych jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Spółkę. Prawnie usprawiedliwionym celem realizowanym przez Spółkę jest ewidencja osób wchodzących do Spółki oraz z niej wychodzących.

Zgodnie z art. 26 ust. 1 pkt 3 ustawy, adekwatność danych, w stosunku do celów, w jakich są przetwarzane powinna być rozumiana jako równowaga pomiędzy prawem osoby do dysponowania swoimi danymi, a interesem administratora danych, który nie może stawiać swego interesu ponad dobro osoby, której dane przetwarza. Dla zachowania równowagi administrator może żądać danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przetwarzane. W ocenie Generalnego Inspektora przetwarzanie przez Spółkę nr PESEL od osób wchodzących do budynku Spółki nie jest niezbędne do osiągnięcia celu przetwarzania danych osobowych. Mając na względzie, że na podstawie nr PESEL można nie tylko potwierdzić tożsamość osoby, której numer ten jest przyporządkowany, ale również ustalić m.in. datę urodzenia tej osoby, należy uznać, iż zakres danych pozyskiwanych przez Spółkę jest zbyt szeroki i nieadekwatny do celu przetwarzania tych danych.

Należy zauważyć, iż za nienaruszające zasady adekwatności zostało uznane odnotowywanie wyłącznie danych w zakresie imienia, nazwiska i numeru dokumentu służącego do identyfikacji osób w celu zapewnienia bezpieczeństwa budynku (wyr. WSA w Warszawie z 12 maja 2005 r., II S.A./Wa 2499/00, niepublikowany).

Ponadto nie można zgodzić się z argumentacją Spółki przedstawioną w piśmie z dnia […] kwietnia 2015 r., iż „jedynie nr PESEL pozwala na wcześniejszą, jednoznaczną weryfikację osoby niepożądanej". Należy podnieś, iż oprócz nr PESEL Spółka przetwarza od osoby wchodzącej na teren Spółki także dane w zakresie: imię, nazwisko, serię i nr dowodu osobistego lub nr prawa jazdy, daną dotyczącą miejsca zatrudnienia osoby wchodzącej na teren Spółki (jeżeli wchodzi na teren Spółki w celach zawodowych) bądź informację, iż jest to osoba prywatna. Ponadto w Spółce na podstawie umowy z dnia […] maja 2012 r. nr […] została zapewniona całodobowa ochrona przez E. Sp. z o. o. (podmiot zawodowo świadczący usługę ochrony osób oraz mienia), który wykonuje swoje zadania m.in. na podstawie wdrożonego w Spółce dokumentu o nazwie „Instrukcja kontroli ruchu osobowego i materiałowego", w sposób szczegółowy regulującego kwestie związane z przebywaniem osób trzecich na terenie Spółki. Ponadto należy zauważyć, iż w Spółce funkcjonuje także system monitoringu wizyjnego, którego głównym celem jest rejestracja ewentualnych naruszeń, a więc identyfikacja osób.

W związku z powyższym należy podnieść, iż obecnie stosowana przez Spółkę praktyka polegająca na przetwarzaniu nr PESEL w celu ewidencji osób wchodzących do budynków Spółki oraz z nich wychodzących jest niezgodna z art. 26 ust. 1 pkt 3 ustawy.

2. Zgodnie z art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Jednocześnie ustalono, iż Spółka nie opracowała procedury dotyczącej usuwania oraz archiwizacji danych przetwarzanych w systemie informatycznym o nazwie A po ustaniu celu, dla którego zostały pozyskane (system kontroli dostępu, w którym przetwarzane są dane osób wchodzących do budynków Spółki).

W piśmie Spółki z dnia […] kwietnia 2015 r. wskazano, iż został opracowany projekt dokumentu o nazwie „Procedura archiwizacji oraz usuwania danych w […]" określającej terminy przechowywania oraz usuwania danych. Jednak wdrożenie procedury wymaga przebudowy systemu informatycznego o nazwie „A". Producent oprogramowania zadeklarował wykonanie niezbędnych zmian w oprogramowaniu w okresie trzech miesięcy od momentu otrzymania zlecenia. Aby Spółka mogła zlecić wykonanie tych prac, niezbędna jest decyzja Generalnego Inspektora Ochrony Danych Osobowych w zakresie przetwarzania przez Spółkę nr PESEL.

Uwzględniając zatem przedstawione wyjaśnienia oraz działania podjęte przez Spółkę odnośnie przywrócenia stanu zgodnego z prawem, Generalny Inspektor Ochrony Danych Osobowych wyznaczył trzymiesięczny termin wykonania niniejszej decyzji w tym zakresie.

Jednocześnie, na podstawie przedstawionych wyjaśnień i innych dowodów w niniejszej sprawie, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj. Spółka:

1) zawarła z E. Sp. z o. o. oraz S. Sp. z o.o. pisemną umowę powierzenia przetwarzania danych osobowych przetwarzanych w systemie monitoringu wizyjnego (art. 31 ust. 1 ustawy),

2) zawarła z E. Sp. z o. o. oraz ED. Sp. z o.o. pisemną umowę powierzenia przetwarzania danych osobowych przetwarzanych w systemie informatycznym o nazwie A (art. 31 ust. 1 ustawy),

3) opracowała procedury określające termin przechowywania (w tym usuwania) danych osobowych (wizerunek) rejestrowanych za pomocą urządzenia technicznego służącego do zapisu obrazu,

4) wskazała w prowadzonym wykazie zbiorów danych osobowych, na który składa się dokument o nazwie „Wykaz zasobów danych osobowych i systemów ich przetwarzania" programy zastosowane do przetwarzania tych danych,

5) zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „B" (zgłoszenie nr R: […]).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Jak stwierdził Naczelny Sąd Administracyjny w uzasadnieniu wyroku z dnia 19 listopada 2001 r. (sygn. akt II SA 2702/00): „(...) skoro w toku prowadzonego (...) postępowania administracyjnego zniesiony został stan naruszenia prawa, którego miało dotyczyć rozstrzygnięcie, to postępowanie stało się bezprzedmiotowe". Ponadto przesłanką umorzenia postępowania na podstawie art. 105 § 1 K.p.a. jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny", czyli 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. SA/Sz. 1029/97).

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

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, 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 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 2014 r. poz. 1619 z późn. zm.).