GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Warszawa 19 października 2017 r.

DIS/DEC- 1270/17/77313

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 2017 r. poz. 1257), art. 12 pkt 2, art. 18 ust. 1 pkt 1 oraz art. 22 w związku z art. 26 ust. 1 pkt 1, art. 31 ust. 1 i art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) a także § 4 pkt 1, pkt 2, pkt 3 i pkt 4 oraz § 5 pkt 4 i pkt 5 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) zwanego dalej także „rozporządzeniem”, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Samodzielny Publiczny Zakład Opieki Zdrowotnej w […] (dalej: SPZOZ),

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

1. Uzupełnienie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityki bezpieczeństwa, w zakresie: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (§ 4 pkt 1 rozporządzenia); wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

(§ 4 pkt 2 rozporządzenia); opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3 rozporządzenia); sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Uzupełnienie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w zakresie: procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia); sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt 4 (§ 5 pkt 5 rozporządzenia), w terminie 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 SPZOZ 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 2016 r. poz. 922) 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). Zakresem kontroli objęto udostępnienie przez SPZOZ danych osobowych osobom nieuprawnionym. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Dyrektora SPZOZ.

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

1. Powierzeniu danych osobowych pacjentów SPZOZ K. Sp. z o.o. (obecna nazwa: T. S.A.) bez zawarcia na piśmie z ww. podmiotem umowy powierzenia przetwarzania danych osobowych (art. 26 ust. 1 pkt 1 ustawy i art. 31 ust. 1 ustawy).

2. Powierzeniu danych osobowych pacjentów SPZOZ A. Sp. z o.o. bez zawarcia na piśmie z ww. podmiotem umowy powierzenia przetwarzania danych osobowych (art. 26 ust. 1 pkt 1 ustawy i art. 31 ust. 1 ustawy).

3. Nieuzupełnienieniu polityki bezpieczeństwa w zakresie: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (§ 4 pkt 1 rozporządzenia); wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (§ 4 pkt 2 rozporządzenia); opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3 rozporządzenia); sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia).

4. Nieuzupełnienieniu instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w zakresie: procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia) oraz sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt 4 (§ 5 pkt 5 rozporządzenia).

W piśmie z dnia […] sierpnia 2017 r. (sygn. […]), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, SPZOZ został poinformowany 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, Dyrektor SPZOZ, pismem z dnia […] września 2017 r. (znak: […]) złożył wyjaśnienia, w których poinformował, że:

1) SPZOZ zawarł w dniu […] lipca 2017 r. umowę powierzenia przetwarzania danych osobowych z T. S.A. […] (poprzednia nazwa: K. Sp. z o.o.),

2) SPZOZ zawarł w dniu […] lipca 2017 r. umowę powierzenia przetwarzania danych osobowych z A. Sp. z o.o. (dowód: kopia powołanych umów),

3) do końca września 2017 r. zostanie uzupełniony dokument o nazwie „Polityka bezpieczeństwa”.

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

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. Dokumentację, o której jest mowa wyżej, zgodnie z ust. 3, wdraża administrator danych.

Natomiast zgodnie z § 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; 2) wykaz zbiorów danych osobowych

wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; 4) sposób przepływu danych pomiędzy poszczególnymi systemami; 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

W toku czynności kontrolnych ustalono, że Zarządzeniem nr […] z dnia […] lipca 2017 r. Dyrektora Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w […] wprowadzona została w SPZOZ dokumentacja o nazwie „Polityka bezpieczeństwa".

Analiza „Polityki bezpieczeństwa" wykazała, że dokumentacja ta nie spełnia wszystkich wymogów, o których mowa w § 4 rozporządzenia, tj.:

1) zawarty w „Polityce bezpieczeństwa" opis obszaru, o którym mowa w § 4 pkt 1 rozporządzenia, sporządzony został w sposób zbyt ogólny. Opis ten zawiera jedynie wskazanie siedziby SPZOZ bez wyszczególnienia budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

2) zawarty w „Polityce bezpieczeństwa" „Rejestr zbiorów danych osobowych" stanowiący wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (o którym mowa w § 4 pkt 2 rozporządzenia) nie zawiera wyszczególnionych wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Ustalono, że rejestr załączony do „Polityki bezpieczeństwa" jest wyciągiem zawierającym część pełnego wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Pełny wykaz prowadzony jest przez Administratora Bezpieczeństwa Informacji w odrębnej, roboczej dokumentacji tzw. dokumentacji wspomagającej,

3) „Polityka bezpieczeństwa" nie zawiera opisu struktury zbiorów danych, wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3 rozporządzenia),

4) „Polityka bezpieczeństwa" nie uwzględnia w sposób prawidłowy wymogu, o którym mowa w § 4 pkt 4 rozporządzenia, tj. nie zawiera informacji o sposobie przepływu danych pomiędzy poszczególnymi systemami. Prowadzona w SPZOZ „Polityka bezpieczeństwa" zawiera jedynie sporządzony w sposób ogólny przykład kierunku przepływu danych dotyczący obszaru finansowo-księgowego, kadrowo-płacowego, bez uwzględnienia innych obszarów przetwarzania i sposobu w jakim ten przepływ się odbywa.

Zgodnie § 5 pkt 4 i pkt 5 rozporządzenia, instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawiera: procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia); sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt 4 (§ 5 pkt 5 rozporządzenia).

W toku kontroli ustalono, że dokument o nazwie „Instrukcja zarządzania systemem

informatycznym ochrony danych osobowych” stanowi integralną część „Polityki bezpieczeństwa”.

Analiza „Instrukcji zarządzania systemem informatycznym ochrony danych osobowych” wykazała, że dokument ten nie zawiera: procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia); sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt 4 (§ 5 pkt 5 rozporządzenia).

W piśmie z dnia […] września 2017 r. Dyrektor SPZOZ m.in. wskazał, że do końca września 2017 r. zostanie uzupełniona dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. dokument o nazwie „Polityka bezpieczeństwa”. Jednakże powołana dokumentacja nie została przesłana do Biura Generalnego Inspektora Ochrony Danych Osobowych dlatego nie można było dokonać oceny czy spełnia ona obecnie wymogi określone w § 4 pkt 1, pkt 2, pkt 3 i pkt 4 rozporządzenia oraz w § 5 pkt 4 i pkt 5 rozporządzenia.

Wobec powyższego Generalny Inspektor nakazał przywrócenie stanu zgodnego z prawem w ww. 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.:

1) dane osobowe pacjentów SPZOZ przekazywane są na podstawie umowy powierzenia przetwarzania danych osobowych T. S.A.,

2) dane osobowe pacjentów SPZOZ przekazywane są na podstawie umowy powierzenia przetwarzania danych osobowych A. Sp. z o.o.

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”.

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. 127 § 3 Kodeksu postępowania administracyjnego w zw. z art. 21 ust. 1 ustawy o ochronie danych osobowych strona niezadowolona z niniejszej decyzji może, w terminie 14 dni od dnia jej doręczenia, złożyć do Generalnego Inspektora Ochrony Danych Osobowych wniosek o ponowne rozpatrzenie sprawy (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00 – 193 Warszawa). W trakcie biegu terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy strona może zrzec się prawa do jego wniesienia wobec organu administracji publicznej, który wydał decyzję. Z dniem doręczenia organowi administracji publicznej oświadczenia o zrzeczeniu się prawa do wniesienia wniosku o ponowne przez ostatnią ze stron postępowania, decyzja staje się ostateczna i prawomocna, co oznacza, że decyzja podlega natychmiastowemu wykonaniu i brak jest możliwości zaskarżenia decyzji do Wojewódzkiego Sądu Administracyjnego. Nie jest możliwe skuteczne cofnięcie oświadczenia o zrzeczeniu się prawa do wniesienia odwołania.

Jeżeli strona nie zamierza korzystać z prawa do zwrócenia się z wnioskiem o ponowne rozpatrzenie sprawy, może wnieść do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na decyzję w terminie 30 dni od dnia doręczenia decyzji stronie. Skargę wnosi się za pośrednictwem Generalnego Inspektora Ochrony Danych Osobowych. Wpis od skargi wynosi 200 złotych. Strona składająca skargę może ubiegać się o przyznanie prawa pomocy, które obejmuje zwolnienie od kosztów sądowych oraz ustanowienie adwokata, radcy prawnego, doradcy podatkowego lub rzecznika patentowego. Prawo pomocy może być przyznane na wniosek strony złożony przed wszczęciem postępowania lub w toku postępowania. Wniosek ten wolny jest od opłat sądowych.