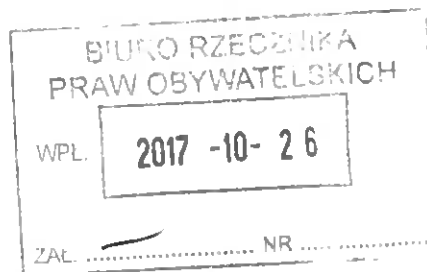




**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**
dr Edyta Bielak - Jomaa



RPW/62635/2017 P
Data: 2017-10-26

Warszawa ²⁴ października 2017 r.

DIS- *78585/17*

dot. VII.520.36.2017.AG

Pan
Adam Bodnar
Rzecznik Praw Obywatelskich
al. Solidarności 77
00-090 Warszawa

Szanowny Pan Prezencie,

w nawiązaniu do pisma Generalnego Inspektora Ochrony Danych Osobowych z dnia 5 lipca 2017 r. (DIS-53434/17) będącego odpowiedzią na pismo z dnia 19 czerwca 2017 r. (sygn. VII.520.36.2017.AG) informuję, że w dniach od 10 do 14 lipca 2017 r. przeprowadzona została kontrola (sygn. DIS-K-421/116/17) 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, poz. 922) 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) w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Kole z siedzibą w Kole przy ul. Księcia Józefa Poniatowskiego 25 (dalej: SPZOZ). Zakresem kontroli objęto udostępnienie przez SPZOZ danych osobowych (pacjentów, pracowników) osobom nieupoważnionym.

W toku przedmiotowych czynności kontrolnych ustalono, że w SPZOZ doszło do naruszenia danych osobowych poprzez udostępnienie danych osobowych (pracowników oraz pacjentów SPZOZ) osobom nieupoważnionym. Jak ustalono w toku kontroli prawdopodobną

przyczyną udostępnienia danych osobowych było niezabezpieczenie przez pracowników SPZOZ serwera w trakcie procesu aktualizacji systemów informatycznych użytkowanych w SPZOZ. Ponadto informuję, że Prokuratura Okręgowa w Koninie prowadzi śledztwo (sygn. PO I Ds. 32.2017) w przedmiocie niezabezpieczenia danych osobowych przed ich zabraniem, uszkodzeniem lub zniszczeniem przez osobę nieuprawnioną, tj. o czyn z art. 52 ustawy o ochronie danych osobowych.

Jednocześnie informuję, że w SPZOZ podjęto następujące środki naprawcze:

- 1) zawieszono pracowników Sekcji Informatycznej SPZOZ w obowiązkach świadczenia pracy z powodu wycieku danych wrażliwych z serwera. Z jednym z pracowników została rozwiązana umowa o pracę,
- 2) podjęto współpracę z podmiotem zewnętrznym, której przedmiotem jest wykonanie zadań i czynności związanych ze sprawowaniem nadzoru nad prawidłowym funkcjonowaniem i zabezpieczeniem sieci IT,
- 3) przeprowadzono audyt systemów informatycznych przez podmiot zewnętrzny. Zakresem objęto sprawdzenie ochrony danych osobowych oraz bezpieczeństwa sieci,
- 4) podmiot zewnętrzny przeprowadził szkolenie, którego zakresem objęto przetwarzanie danych osobowych oraz związane z nim zagrożenia,
- 5) dokonano aktualizacji poczty służbowej pracowników SPZOZ z uwzględnieniem obecnego stanu zatrudnienia i zakresu sprawowanych funkcji,
- 6) powołano Administratora Systemów Informatycznych,
- 7) zabezpieczono serwer, w którym przetwarzane są dane osobowe pacjentów oraz pracowników SPZOZ poprzez: zmianę wszystkich haseł użytkowników systemów informatycznych, wyłączenie części interfejsów sieciowych oraz usługi poczty elektronicznej. Usługa ta przeniesiona została na inny serwer,
- 8) opracowano procedury reagowania na naruszenie danych osobowych,
- 9) zawarto umowy powierzenia przetwarzania danych osobowych z podmiotami, z którymi podpisano umowy na wykonywanie świadczeń zdrowotnych.

Nadto informuję, że w dniu 19 października 2017 r. Generalny Inspektor Ochrony Danych Osobowych wydał wobec SPZOZ decyzję nakazującą przywrócenie stanu zgodnego z prawem (sygn. DIS/DEC-1270/17/77313) poprzez 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 i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

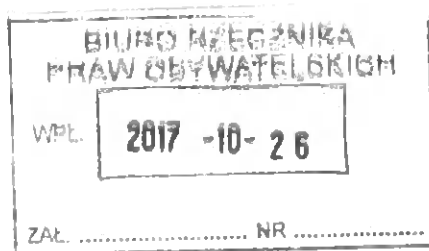
2 wyznaczeni pracownicy
Z up. Generalnego Inspektora
Ochrony Danych Osobowych
Z-ca Dyrektora Departamentu Inspekcji
Dorota Kosacka
Dorota Kosacka



**BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH**

**ul. Stawki 2
00-193 Warszawa**

OPLATA POBRANA
TAXE PERCUE - POLOGNE
umowa z Poczta Polska S.A.
ID nr 299596/W



R



(00)959007734536870540

(00)959007734536870540

SZ. P.

**Bodnar Adam
Rzecznik Praw Obywatelskich
Biuro Rzecznika Praw Obywatelskich
Al. Solidarności 77
00-090 Warszawa
Polska**



16