



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*dr Wojciech R. Wiewiórowski*

Warszawa, dnia 12 sierpnia 2014 r.

DIS/DEC-797/14/62554

dot. [...]

**DECYZJA**

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz § 4 pkt 3 i 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania przez M. danych osobowych,

**Nakazuję M. usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez uzupełnienie polityki bezpieczeństwa obowiązującej w M. jako dokument o nazwie „[...]” o opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, uwzględniający system informatyczny o nazwie „[...]” (system „[...]”), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili w M., zwanym dalej M., kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. kontroli [...]), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), zwaną dalej „ustawą”, i 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 dane osobowe przetwarzane przez M. w ramach wymiany z [...] informacji o osobach zarejestrowanych jako [...] lub [...], które korzystają ze świadczeń [...] lub ubiegają się o takie świadczenie. W toku kontroli odebrano od pracowników M. 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 p.o. Dyrektora M.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych M., jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na niezawarcie w polityce bezpieczeństwa obowiązującej w M. jako dokument o nazwie „[...]” opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, tj. elementów wymaganych przez § 4 pkt 3 i 4 rozporządzenia.

W związku z powyższym, w dniu [...] lipca 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. Dyrektora M. pismem z dnia [...] lipca 2014 r., nr [...], złożył wyjaśnienia, w których poinformował o uzupełnieniu dokumentu o nazwie „[...]” o opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Ponadto, do pisma z dnia [...] lipca 2014 r., nr [...], p.o. Dyrektora M. przedstawił 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 § 4 pkt 3 i 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Przeprowadzona kontrola wykazała, że obowiązująca w M. polityka bezpieczeństwa w formie dokumentu o nazwie „[...]” nie zawiera opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, tj. elementów wymaganych przez ww. przepis rozporządzenia.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego p.o. Dyrektora M. poinformował, że wskazany dokument został uzupełniony o te elementy, co miały potwierdzić dowody załączone do pisma z dnia [...] lipca 2014 r., nr [...]. Analiza przedstawionych przez p.o. Dyrektora M. dokumentów o nazwach „[...]” oraz „[...]” wykazała, że nie został w nich uwzględniony system informatyczny o nazwie „[...]”, który jest wykorzystywany przez M. do przetwarzania danych osobowych. Nie można zatem uznać, że w zakresie objętym niniejszym postępowaniem został przywrócony stan zgodny z prawem.

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

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych i 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 2005 r., Nr 229, poz. 1954 z późn. zm.).