



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*dr Wojciech R. Wiewiórowski*

Warszawa, dnia 1 lutego 2011 r.

DIS/DEC-56/4114/11

dot. [...]

**D E C Y Z J A**

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz w związku z § 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 danych osobowych przez N. Sp. z o.o.,

**nakazuję N. Sp. z o.o., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez zapewnienie, aby polityka bezpieczeństwa zawierała: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami oraz określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

## Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w N. Sp. z o.o., zwanej dalej Spółką, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. [...], 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, 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. W toku kontroli odebrano od pracowników Spółki 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 Prezesa Zarządu Spółki.

Na podstawie całokształtu materiału dowodowego zgromadzonego w toku kontroli ustalono, że w procesie przetwarzania danych Spółka, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia polegały na braku w polityce bezpieczeństwa: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych, opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi, sposobu przepływu danych pomiędzy poszczególnymi systemami; określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (§ 4 rozporządzenia).

W piśmie z dnia [...] grudnia 2010 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. Spółka nie skorzystała z prawa złożenia wyjaśnień oraz nie przedstawiła dowodów mogących 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 art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1 ustawy. 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, zwana dalej „instrukcją”. Zgodnie z § 3 ust.2 rozporządzenia, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych. Zgodnie z § 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Z ustaleń kontroli wynika, iż opracowana i wdrożona przez Spółkę jako administratora danych osobowych polityka bezpieczeństwa nie spełnia wymogów określonych w § 4 rozporządzenia gdyż nie zawiera: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych, opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi, sposobu przepływu danych pomiędzy poszczególnymi systemami; określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

Decyzja jest ostateczna. 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.