



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

DOLiS-035- 3755/13

Warszawa, dnia maja 2014 r.

Prezesa Zarządu

W związku z Pana pismem, które wpłynęło do Biura Generalnego Inspektora Ochrony Danych Osobowych w dniu 20 stycznia 2014 r., będącym odpowiedzią na wystąpienie Generalnego Inspektora Ochrony Danych Osobowych z dnia 19 grudnia 2013 r., uprzejmie dziękuję za przedstawione informacje dotyczące sposobu weryfikacji klientów przez P.

W opinii Generalnego Inspektora Ochrony Danych Osobowych, klient powinien mieć możliwość wyboru identyfikującej go danej, przy każdej okazji nawiązywania kontaktu z biurem obsługi klienta, a zatem bez obowiązku podawania numeru PESEL lub numeru dokumentu tożsamości (które to dane są ściśle związane z prywatnością osoby fizycznej) dla potrzeb identyfikacji.

Mocą art. 26 ust. 1 ustawy o ochronie danych osobowych, 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 (pkt 1), zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 (pkt 2), merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (pkt 3). Omawiany przepis (pkt 2 i 3) statuuje zasadę adekwatności przetwarzania danych osobowych. Zgodnie z nią, przetwarzane (gromadzone) dane nie powinny wykraczać swym rodzajem i swą treścią poza potrzeby wynikające z celu ich zbierania, a zatem dla określonych celów powinny być przetwarzane tylko dane niezbędne i proporcjonalne do celu ich przetwarzania.

Zgodnie z art. 36 ust 1 ustawy o ochronie danych osobowych, każdy 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, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Przytoczony przepis zobowiązuje każdego administratora danych do wprowadzenia takich środków oraz rozwiązań technicznych i organizacyjnych, które zapewnią danym osobowym, w konkretnych warunkach i okolicznościach przetwarzania, skuteczną ochronę przed potencjalnymi zagrożeniami, w tym pozostającymi w związku z zakresem przetwarzanych danych osobowych.