



**GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH**

Dr Wojciech R. Wiewiórowski

Warszawa, dnia 29 marca 2013 r.

GI-035-3/13

**Pan
Andrzej Jakubiak
Przewodniczący Komisji
Nadzoru Finansowego
Plac Powstańców Warszawy 1
00-950 Warszawa**

W Y S T Ą P I E N I E

Działając na podstawie art. 19a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zwanej dalej ustawą o ochronie danych osobowych, zgodnie z którym w celu realizacji zadań, o których mowa w art. 12 pkt. 6, Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych, uprzejmie proszę Pana Przewodniczącego o podjęcie działań mających na celu ocenę zagrożeń prawnych i faktycznych spowodowanych wprowadzaniem przez instytucje bankowe kart płatniczych wyposażanych w moduły płatności „zbliżeniowych”, podczas gdy technologia ta budzi wiele wątpliwości w zakresie dotyczącym bezpieczeństwa przetwarzanych przy jej zastosowaniu danych.

W szczególności proszę Pana Przewodniczącego o:

- przeprowadzenie analizy wpływu zastosowanych rozwiązań wykorzystujących technologię kart zbliżeniowych na ochronę danych osobowych w poszczególnych

zastosowaniach wykonaną zgodnie z zaleceniami środowiska producentów kart wyposażonych w moduł RFID, o której mowa w opinii 9/2011 Grupy Roboczej Art. 29 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID oraz

- przeprowadzenie analizy zgodności z rekomendacjami zawartymi w znowelizowanej Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach przyjętej w dniu 8 stycznia 2013 r. przez Komisja Nadzoru Finansowego.**

Generalny Inspektor Ochrony Danych Osobowych z dużym niepokojem śledzi przekazywane w prasie i mediach elektronicznych informacje na temat możliwości nieuprawnionego pozyskania danych osobowych właścicieli kart płatniczych wyposażonych w technologię NFC stanowiącą odmianę technologii RFID o ograniczonym do niewielkich odległości zasięgu oraz możliwościach jednoczesnego odbioru i nadawania sygnałów, co czyni ją bardziej odporną na kolizje¹. Moduły NFC stosowane w kartach płatniczych są modułami pasywnymi, a odczytywane z nich lub zapisywane na nich dane nie są zabezpieczane kryptograficznie co stanowić może potencjalne źródło nieuprawnionego dostępu do danych lub nieuprawnionej ingerencji w ich treść. W serwisach internetowych poświęconych bezpieczeństwu informacyjnemu^{2,3} pojawiło się szereg informacji o możliwości odczytu danych z takich kart przez nieuprawnione osoby, a nawet o możliwościach ich sklonowania przez nieuprawnione osoby a następnie użycia tych klonów do wykonania płatności za zakupy. Potwierdzeniem takiej podatności na ataki są prezentowane nagrania wideo, na których pokazuje się, że przy użyciu czytnika, z kart płatniczych wyposażonych w moduł RFID można odczytać wiele z zapisanych na niej danych z odległości około 10 cm od karty.

Jednocześnie pojawiają się informacje o wprowadzaniu przez podmioty rynkowe rozwiązaniach polegających na integracji kart płatniczych z kartami SIM do telefonów komórkowych, umożliwiających wykonywanie transakcji płatniczych poprzez zbliżenie telefonu komórkowego do czytnika. Jest to możliwe przy użyciu telefonów wyposażonych w technologię NFC. Świadczenie takich usług rozpoczynają w Polsce operator telefonii komórkowej Orange we

¹ Ekta Desai, Mary Grace Shajan, "A Review on the Operating Modes of Near Field Communication" in International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012, <http://www.ijeat.org/attachments/File/v2i2/B0956112212.pdf>.

² Marcin Chmielewski „Internetowi sprzedawcy oferują klonowanie kart zbliżeniowych”, tekst dostępny jest na: <http://www.chip.pl/news/bezpieczenstwo/technologie-bezpieczenstwa/2011/12/internetowi-sprzedawcy-oferuja-klonowanie-kart-zblizeniowych>

³ Vi. Curry, „Odczytywanie zbliżeniowych kart kredytowych (RFID)”, tekst dostępny jest na: <http://niebezpiecznik.pl/post/klonowanie-zblizeniowych-kart-kredytowych-rfid/>

współpracy z MasterCard i mBankiem⁴ oraz operator telefonii komórkowej T-Mobile we współpracy z mBankiem (usługa MyWallet)⁵. Zastosowanie telefonów wyposażonych w technologię NFC, jak donoszą media daje ponadto nieograniczoną możliwość „wydłużenia” odległości z jakiej terminal może odczytać dane z karty zbliżeniowej nieświadomego „płatnika”⁶. Używając 2 telefonów wyposażonych w technologię NFC z odpowiednimi aplikacjami, osoba A może wówczas zapłacić za swoje zakupy kartą zbliżeniową przypadkowej osoby w autobusie lub innym zatłoczonym miejscu, u której osoba B współpracująca z osobą A wykryła kartę płatniczą. Zainstalowana w telefonie osoby A aplikacja połączona przed wykonaniem płatności z telefonem osoby B spowoduje, że do płatności wykorzystane zostaną dane z karty zbliżeniowej, którą „widzi” telefon osoby B.

Z informacji podanej przez Grupę Roboczą ds. Technologii przy Federalnym Rzeczniku Ochrony Danych oraz Rzecznikach Landowych Republiki Federalnej Niemiec, wynika, że na stosowanych w Niemczech kartach płatniczych mogą być zapamiętywane logi kilku ostatnich transakcji ładowania/rozładowania karty oraz informacje o wykonanych w ostatnim okresie co najmniej 15 transakcjach płatniczych, zawierające takie dane jak: czas wykonania transakcji, numer karty sprzedawcy (retailer credit card), kwota transakcji oraz pozostała kwota wolnych środków. Wymienione dane, jak wynika z raportu wspomnianej Grupy Roboczej można odczytać z karty debetowej klienta wyposażonej w moduł płatności zbliżeniowej bez żadnych dodatkowych autoryzacji przez jej posiadacza.

Ponadto jak wynika z sygnalizowanych przez posiadaczy tych kart opisów zdarzeń, transakcje wykonywane tymi kartami są realizowane w trybie offline, co powoduje, że wprowadzone przez wydające je instytucje ograniczenia limitu dziennych transakcji dla kwot poniżej 50 zł, dla których płatności realizowane są bez autoryzacji, nie są skuteczne^{7,8,9}. Opisy te wskazują, że istnieje sprzeczność między wyjaśnieniami banków¹⁰ dotyczącymi limitów transakcji, w których zapewnia się klientów o bezpieczeństwie kart zbliżeniowych, w tym ustanowionych limitach transakcji, a istniejącą rzeczywistością.

⁴ Aleksandra Stanisławska, teks dostępny jest na: <http://www.ekonomia24.pl/artukul/942578.html>

⁵ Paweł Krzyżanowski, teks dostępny jest na: <http://www.komputerswiat.pl/nawosci/wydarzenia/2012/45/t-mobile-mywallet-od-dzis-dla-klientow-mbanku.aspx>

⁶ Niebezpiecznik.pl, „Uniwersalny atak na karty zbliżeniowe”, teks dostępny jest na: <http://niebezpiecznik.pl/post/uniwersalny-atak-na-karty-zblizeniowe/?more>

⁷ Polacy wrobieni w karty zbliżeniowe. To raj dla złodziei, teks dostępny jest na: <http://www.sfora.biz/Polacy-wrobieni-w-karty-zblizeniowe-To-raj-dla-zlodziei-a52687>

⁸ Maciej Samcik, „Kradzież bezdotykowa. Czy karty zbliżeniowe są dobrze zabezpieczone”, teks dostępny jest na: http://wyborcza.biz/finanse/1,105684,13417209,Kradziez_bezdotykowa__Czy_karty_zblizeniowe_sa_dobrze.html#MT

⁹ Maciej Samcik, Kradzieże z kart zbliżeniowych możliwe dlatego, że banki... chciały przyoszczędzić?, teks dostępny jest na: <http://samcik.blox.pl/2013/02/Kradzieze-z-kart-zblizeniowych-mozliwe-dlatego-ze.html>

¹⁰ Maciej Kielczarek, „Bezpieczeństwo kart zbliżeniowych”, teks dostępny jest na: <http://www.mbank.pl/porozmawiajmy/blog/artukul,1109,bezpieczenstwo-kart-zblizeniowych.html>

Z powyższego wynika, że wprowadzana powszechnie przez instytucje finansowe technologia kart zbliżeniowych nie jest wystarczająco dopracowana zarówno technologicznie jak i organizacyjnie i wymaga dokładnej analizy, o czym ostrzegła Komisja Europejska wydając w dniu 12 maja 2009 r. zalecenie w sprawie wdrożenia zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową¹¹.

Wymienione właściwości kart płatniczych wyposażonych w funkcje płatności zbliżeniowych sprawiają, że dane dotyczące jej posiadacza mogą być przetwarzane z naruszeniem zasad bezpieczeństwa danych osobowych wynikających z obowiązujących przepisów prawa, w tym ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (tekst jednolity: Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.). Na uwagę zasługuje w szczególności fakt wykorzystywania w tych kartach technologii RFID, dla której, w przypadku jej zastosowania, Komisja Europejska zaleciła przeprowadzanie analizy wpływu wprowadzanych rozwiązań na ochronę prywatności, o czym wspomniano wyżej¹¹. W zaleceniu tym Komisja wprowadziła wymóg zatwierdzenia przez Grupę Roboczą ds. Ochrony Danych ustanowioną na mocy art. 29 Dyrektywy 95/46/WE, zwaną dalej Grupą Roboczą Art 29, opracowanych przez sektor ram oceny skutków w zakresie ochrony danych osobowych i prywatności w zastosowaniach RFID. Dokument taki o nazwie „Ramy oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID”, został przez sektor producentów i dostawców technologii RFID opracowany i zatwierdzony przez ww. Grupę Roboczą Art. 29¹² w dniu 11 lutego 2011 r. Dokument ten dostępny jest w polskiej wersji językowej na stronie internetowej pod adresem: http://ec.europa.eu/information_society/policy/rfid/documents/pia-pl.pdf. Zgodnie z opinią Grupy Roboczej, Art. 29 nr 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID, dokument ten powinien stać się skuteczny nie później niż po okresie 6 miesięcy od jego opublikowania, czyli nie później niż od 12 lutego 2012 r.

Zagrożenia ochrony danych osobowych w związku z wprowadzeniem do stosowania przez instytucje finansowe kart kredytowych i/lub debetowych wyposażonych w moduł płatności zbliżeniowych jak wynika ze wskazanych we wstępie informacji należy rozważyć w dwóch następujących kategoriach:

¹¹ Dziennik Urzędowy Unii Europejskiej L 122/47: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:PL:PDF>

¹² Opinia 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID Przyjęta w dniu 11 lutego 2011 r. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_pl.pdf

1. możliwości nieuprawnionego ujawnienia danych osobowych posiadaczy kart zbliżeniowych w zakresie: imienia, nazwiska, numeru karty kredytowej, daty jej wydania, a w niektórych przypadkach również informacje o kilku ostatnio dokonanych transakcjach, oraz
2. możliwości narażenia posiadaczy kart zbliżeniowych na straty finansowe w przypadku jej zagubienia, kradzieży lub stania się ofiarą zorganizowanego przestępstwa wykorzystującego możliwości opisane na portalu niebezpiecznik.pl w artykule pod adresem:

<http://niebezpiecznik.pl/post/universalny-atak-na-karty-zblizeniowe/>

Z publikowanych właściwości kart płatniczych wyposażanych w moduły płatności zbliżeniowych oraz stosowanych powszechnie systemów płatności wyposażonych w czytniki kart zbliżeniowych wynika, że zarówno odczyt danych dotyczących uprawnionego posiadacza takiej karty, jak i wykonanie transakcji płatniczej przy jej użyciu, jeżeli kwota transakcji nie przekracza określonej wielkości np. 50 lub 100 zł. możliwy jest bez żadnej autoryzacji jej posiadacza. Opisano ponadto scenariusze, które pokazują, że odczyt danych dotyczących właściciela takiej karty płatniczej, a nawet wykonanie transakcji przy jej użyciu na kwotę nie przekraczającą wyznaczonego przez bank limitu, może być wykonane bez wiedzy i zgody osoby będącej jej właścicielem. Przy czym operacje, o których mowa mogą być wykonane nawet wtedy, gdy uprawniony właściciel karty nadal jest w jej posiadaniu i cały czas stosował się do zaleceń w zakresie bezpieczeństwa ich wykorzystywania wydawanych przez banki.

Zastosowane w systemach wykorzystujących zbliżeniowe karty płatnicze techniczne i organizacyjne rozwiązania mające na celu zapewnienie weryfikacji tożsamości posługujących się nimi osób, jak również rozwiązania dotyczące bezpieczeństwa danych oraz środków klientów – uprawnionych posiadaczy tych kart - nie spełniają w opinii GODO wymagań wskazanych w znowelizowanej *Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach* przyjętej w dniu 8 stycznia 2013 r. przez Komisja Nadzoru Finansowego¹³. Zastosowane w systemach płatności kartami zbliżeniowymi rozwiązania nie są zgodne w szczególności z rekomendacjami 16.1 i 16.4 ww. dokumentu odnoszącymi się odpowiednio do weryfikacji tożsamości uczestników transakcji i uniemożliwiania nieuprawnionego dostępu do danych, w tym minimalizacji prawdopodobieństwa przypadkowego zainicjowania transakcji przez upoważnionych użytkowników. Opisane incydenty i zagrożenia pozwalają również na stwierdzenie, że nie w pełni wykonane zostały zalecenia zawarte w rekomendacji 18.7 odnoszącej się do wdrożenia nowych technologii (w tym płatności wykorzystujących komunikację bliskiego zasięgu oraz bankowości mobilnej) oraz rekomendacji

¹³ Komisja Nadzoru Finansowego, „Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach”, http://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_tcm75-33016.pdf

21.1 odnoszącej się do zapewnienia zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banków z wymaganiami prawnymi, w tym wymaganiami ustawy o ochronie danych osobowych.

Jednocześnie, proszę Pana Przewodniczącego o udzielenie odpowiedzi w przedmiotowej sprawie **w terminie 30 dni** od daty otrzymania niniejszego wystąpienia, albowiem art. 19a ust. 3 ustawy o ochronie danych osobowych stanowi, że podmiot, do którego zostało skierowane wystąpienie lub wnioski, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania.

Informuję przy tym, iż treść niniejszego wystąpienia wraz z udzieloną odpowiedzią opublikowane będą na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych www.giodo.gov.pl.

Do wiadomości:

1. Pan Krzysztof Pietraszkiewicz – Prezes Związku Banków Polskich, ul. Kruczkowskiego 8, 00-380 Warszawa