BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

Departament Inspekcji

Zestawienie wyników sprawdzeń zgodności przetwarzania danych z przepisami o ochronie danych osobowych, które zostały przeprowadzone przez administratorów bezpieczeństwa informacji w bankach w zakresie zabezpieczenia danych osobowych

- Warszawa, 2017 r. -

I. Wprowadzenie

Generalny Inspektor Ochrony Danych Osobowych zwrócił się, na podstawie art. 19b ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), zwanej dalej „ustawą", do administratorów bezpieczeństwa informacji w 12 bankach, w tym w Narodowym Banku Polskim i 8 bankach spółdzielczych, o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą o ochronie danych osobowych 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), zwanego dalej „rozporządzeniem", w tych podmiotach.

Zakresem sprawdzeń objęto przetwarzanie danych osobowych przez banki w zakresie ich zabezpieczenia, **w szczególności ustalenie:**

1) jakie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną zostały zastosowane przez administratora danych, a w szczególności, w jaki sposób ww. administrator danych zabezpieczył dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy);

2) czy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy, a jeżeli tak, czy dokumentacja ta została wdrożona i spełnia wymogi, o których mowa w § 4 i 5 rozporządzenia (art. 36 ust. 2 ustawy);

3) czy zostały nadane przez administratora danych upoważnienia osobom dopuszczonym do przetwarzania danych osobowych (art. 37 ustawy);

4) czy jest prowadzona ewidencja osób upoważnionych do przetwarzania danych i czy spełnia wymogi określone w art. 39 ust. 1 ustawy;

5) w jaki sposób administrator danych sprawuje kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy);

6) czy administrator danych powierzył przetwarzanie danych osobowych innym podmiotom, a jeżeli tak, jakim podmiotom i na podstawie jakich umów (art. 31 ustawy);

7) w jakich systemach informatycznych są przetwarzane dane osobowe oraz jaki poziom bezpieczeństwa przetwarzania danych, powinien być w nich zastosowany, stosownie do § 6 rozporządzenia;

8) czy systemy informatyczne służące do przetwarzania danych osobowych spełniają wymogi określone w rozporządzeniu, tj.:

a) czy dla każdej osoby, której dane osobowe są przetwarzane w systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie: daty pierwszego wprowadzenia danych do systemu; identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba; źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych; sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy (§ 7 ust. 1 rozporządzenia);

b) czy odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych (§ 7 ust. 2 rozporządzenia);

c) czy dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 8a (§ 7 ust. 3 rozporządzenia);

d) czy obszar, w którym przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych (pkt I ust. 1 części A załącznika do rozporządzenia);

e) czy przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych (pkt I ust. 2 części A załącznika do rozporządzenia);

f) czy w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych, to jest czy każdy użytkownik systemu informatycznego posiada odrębny identyfikator, a dostęp do danych osobowych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia (pkt II części A załącznika do rozporządzenia);

g) czy systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (pkt III części A załącznika do rozporządzenia);

h) jeżeli uwierzytelnienie użytkowników w systemie informatycznym następuje za pomocą hasła, jak często następuje jego zmiana oraz z ilu i jakich składa się znaków (pkt IV ust. 1 i 2 części A oraz pkt VIII części B załącznika do rozporządzenia);

i) czy dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych;

j) czy kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności (pkt IV ust. 3 i ust. 4 części A załącznika do rozporządzenia);
k) czy zostały opracowane i wdrożone procedury dotyczące sposobu postępowania z komputerami przenośnymi oraz nośnikami danych zawierającymi dane osobowe podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych (pkt V części A załącznika do rozporządzenia);
l) czy zostały opracowane i wdrożone procedury dotyczące sposobu postępowania z urządzeniami, dyskami lub innymi elektronicznymi nośnikami informacji, zawierającymi dane osobowe, przeznaczonymi do likwidacji, przekazania podmiotowi nieuprawnionemu do przetwarzania danych lub naprawy (pkt VI części A załącznika do rozporządzenia);
ł) czy administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego (pkt VII części A załącznika do rozporządzenia);
m) czy urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych (pkt IX części B załącznika do rozporządzenia);
n) w jaki sposób system informatyczny służący do przetwarzania danych osobowych jest chroniony przed zagrożeniami pochodzącymi z sieci publicznej (pkt XII części C załącznika do rozporządzenia);
o) czy administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej (pkt XIII części C załącznika do rozporządzenia).

Sprawdzenia zostały przeprowadzone w okresie od grudnia 2015 r. do lutego 2016 r.

II. Zagadnienie problemowe

Duża liczba otrzymywanych od ABI sprawozdań z ww. sprawdzeń nie zawierała wszystkich niezbędnych informacji i dowodów potwierdzających dokonane ustalenia. W związku z tym konieczne było zwracanie się przez inspektorów na piśmie (często wielokrotne) do administratorów bezpieczeństwa informacji o złożenie dodatkowych wyjaśnień i dowodów, niezbędnych do dokonania oceny przez inspektorów, czy przetwarzanie danych osobowych w zakresie objętym sprawdzeniem odbywa się zgodnie z przepisami o ochronie danych osobowych.

Zdarzało się, iż sprawozdania, jak również wyjaśnienia, były przesyłane do Generalnego Inspektora Ochrony Danych Osobowych bezpośrednio przez ABI, a nie za pośrednictwem administratorów danych, czego wymaga art. 19b ust. 2 ustawy o ochronie danych osobowych[1].

Treść sprawozdań wskazywała niejednokrotnie na niepełną wiedzę w zakresie ochrony danych osobowych u administratorów bezpieczeństwa informacji niezbędną do prawidłowego sporządzenia sprawozdania ze sprawdzenia. ABI częstokroć wskazywali w sprawozdaniach, iż nie stwierdzili nieprawidłowości w procesie przetwarzania danych osobowych, podczas gdy z analizy dokumentacji ze sprawdzeń wynikało, że takie nieprawidłowości miały miejsce.

Z informacji przesyłanych przez ABI wynikało również, iż nie identyfikują w sposób prawidłowy obowiązków ciążących na administratorze danych, np. w przypadku, gdy do przetwarzania danych był wykorzystywany system informatyczny udostępniony przez inny podmiot, uznano że administrator danych nie odpowiada za zabezpieczenie danych osobowych przetwarzanych w tym systemie. Przepisy o ochronie danych osobowych nie przewidują, aby administrator danych osobowych mógł być zwolniony z obowiązku odpowiedniego zabezpieczenia danych osobowych, wskazanego w art. 36 ust. 1 ustawy[2], których jest administratorem, w przypadku, gdy do przetwarzania tych danych wykorzystuje system informatyczny udostępniony przez inny podmiot.

Zdarzyło się także, że ABI stwierdził, iż bank spółdzielczy, w którym dokonał sprawdzenia, nie jest administratorem danych przetwarzanych w systemie informatycznym wykorzystywanym do przetwarzania danych osobowych pracowników. Nie ulega natomiast wątpliwości, iż bank, jako pracodawca, decyduje o tym, w jaki sposób i w jakim celu przetwarza dane osobowe pracowników, a tym samym jest administratorem danych osobowych w rozumieniu art. 7 pkt 4 ustawy[3].

III. Podsumowanie wyników sprawdzeń

3.1. Ogólna ocena kontrolowanej działalności

Inspektorzy GIODO, oceniając wyniki przeprowadzonych przez ABI sprawdzeń stwierdzili, iż w zakresie objętym sprawdzeniami większość banków zabezpieczyła dane osobowe w sposób spełniający wymogi określone w przepisach o ochronie danych osobowych.

3.2. Synteza wyników sprawdzeń

[1] Art. 19b ust. 2 Po dokonaniu sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a.

[2] Art. 36 ust. 1 ustawy 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

[3] Art. 7 pkt 4 Przez administratora danych rozumie się organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.

3.2.1. Na podstawie informacji zawartych w sprawozdaniach ze sprawdzeń i załączonych do nich dowodów inspektorzy uznali, iż niektóre z banków naruszyły przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1) niezapewnieniu przez niektóre z systemów informatycznych służących do przetwarzania danych osobowych odnotowania wszystkich lub niektórych informacji wskazanych w § 7 ust. 1 rozporządzenia, jak również sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie ww. informacje (§ 7 ust. 1 i 3 rozporządzenia[4]);

2) niezawarciu 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 tych danych; opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami (w związku z § 4 rozporządzenia[5]).

Wobec ww. podmiotów Generalny Inspektor Ochrony Danych Osobowych wszczął postępowania administracyjne. Wobec tych banków, które usunęły uchybienia w toku prowadzonego postępowania administracyjnego, zostały wydane decyzje administracyjne umarzające postępowanie, natomiast wobec banku, który nie usunął uchybień, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną nakazującą przywrócenie stanu zgodnego z prawem.

3.2.2. Administrator bezpieczeństwa informacji jednego z banków stwierdził naruszenie przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem polegające na niezabezpieczeniu danych przetwarzanych w trzech systemach informatycznych przed utratą integralności oraz poufności. Ponadto uznał, iż niektóre z systemów informatycznych służących do przetwarzania danych osobowych nie spełniały wymogów określonych w § 7 rozporządzenia, tj. nie zapewniały odnotowania wszystkich lub niektórych informacji wskazanych w § 7 ust. 1 rozporządzenia, jak również nie zapewniały sporządzenia i wydrukowania raportu zawierającego w powszechnie

[4] § 7 ust. 1 rozporządzenia Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie: daty pierwszego wprowadzenia danych do systemu; identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba; źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych; sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
§ 7 ust. 2 rozporządzenia Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
§ 7 ust. 3 rozporządzenia Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

[5] § 4 rozporządzenia Polityka bezpieczeństwa 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 tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
.

zrozumiałej formie powyższe informacje. Inspektorzy, na podstawie przedstawionych przez ABI dowodów uznali, że powyższe naruszenia zostały usunięte, i w związku z tym nie zachodziła konieczność wszczęcia postępowania administracyjnego w tym zakresie.