GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 31 maja 2012 r.

DIS/DEC-494/12/34109

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1, art. 22 w związku z art. 7 pkt 5, art. 23 ust. 1 pkt 1, art. 24 ust. 1 pkt 2, pkt 4, art. 26 ust. 1 pkt 3 i pkt 4, art. 31 ust. 1 i ust. 2, art. 37, art. 38, art. 39 ust. 1, art. 41 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 § 4 pkt 1, pkt 2, pkt 3 i pkt 4, § 5 pkt 1, pkt 2, pkt 3, pkt 4, pkt 5, pkt 7 i pkt 8, § 7 ust. 1 pkt 2, ust. 2 i ust. 3 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 B. Sp. z o.o.,

I. Nakazuję B. Sp. z o.o., jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1) **określenie w umowie powierzenia przetwarzania danych zawartej z BZ. S.A., dotyczącej korzystania z systemu informatycznego o nazwie „A" (służącego do przetwarzania danych osobowych osób dokonujących transakcji), zakresu i celu powierzenia danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna;**
2) **zawarcie w polityce bezpieczeństwa informacji, o których mowa w § 4 pkt 1, pkt 2, pkt 3 i pkt 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), tj. wykazu 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, w tym systemu informatycznego o nazwie „A", służącego do przetwarzania danych osobowych osób dokonujących transakcji; opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna;

3) **zapewnienie, aby system informatyczny o nazwie „B", służący do przetwarzania danych osób reprezentujących klientów B. Sp. z o.o., dla każdej osoby, której dane osobowe są przetwarzane w ww. systemie informatycznym zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1, w tym o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w B. Sp. z o.o. (zwaną dalej Spółką), kontrole 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. Zakresem kontroli objęto przetwarzanie przez B. Sp. z o.o. danych osobowych, w tym danych przetwarzanych w związku z prowadzeniem rejestru, o którym mowa w art. 8 ust. 4 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r., Nr 46, poz. 276 z późn. zm.), z wyłączeniem danych pracowników i kandydatów do pracy. 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 tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółka, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1) niezapewnieniu osobom reprezentującym podmioty gospodarcze, będące klientami B. Sp. z o.o., którzy wypełniają formularz wniosku o przyznanie limitu faktoringowego, swobody wyrażenia: zgody na przetwarzanie ich danych osobowych dla celów związanych z działalnością spółki, zgody na udostępnienie danych przez B. Sp. z o.o. podmiotom należącym do Grupy Kapitałowej […], zgody na udostępnienie danych przez podmioty Grupy Kapitałowej […] na rzecz B. Sp. z o.o. (art. 7 pkt 5, art. 23 ust. 1 pkt 1 ustawy);
2) niedopełnianiu obowiązku informacyjnego wobec osób reprezentujących podmioty gospodarcze, będące klientami B. Sp. z o.o., w zakresie informowania o celu udostępniania ich danych *„podmiotom należącym do Grupy Kapitałowej […] ”* oraz o celu pozyskiwania ich danych od *„podmiotów Grupy Kapitałowej […]”*, a także o celu przetwarzania danych, tj. celu rozpatrzenia wniosku i zawarcia umowy faktoringu (art. 24 ust. 1 pkt 2 ustawy);
3) niedopełnianiu obowiązku informacyjnego wobec osób reprezentujących podmioty gospodarcze, będące klientami B. Sp. z o.o., w zakresie informowania o podstawie prawnej pozyskiwania danych, tj. ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. nr 46, poz. 276 ze zm.) (art. 24 ust. 1 pkt 4 ustawy);
4) niezapewnieniu, aby dane w zakresie: nazwiska rodowego, imion rodziców, miejsca urodzenia, płci, wzrostu, koloru oczu, wizerunku, osób reprezentujących klientów B. Sp. z o.o., były przetwarzane adekwatnie w stosunku do celów, w jakich są gromadzone, tj. zawarcia i realizacji umowy faktoringu i realizacji przepisów ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (art. 26 ust. 1 pkt 3 ustawy);
5) niezapewnieniu, aby dane poręczycieli, w zakresie: nazwiska rodowego, imion rodziców, miejsca urodzenia, płci, wzrostu, koloru oczu, wizerunku były przetwarzane adekwatnie w stosunku do celów, w jakich są gromadzone, tj. zawarcia i realizacji umowy faktoringu i realizacji przepisów ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (art. 26 ust. 1 pkt 3 ustawy);

6) niezapewnieniu, aby dane osób reprezentujących podmioty gospodarcze, będące klientami B. Sp. z o.o., oraz poręczycieli były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, w przypadku gdy umowa nie zostanie zawarta, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, tj. rozpatrzenia wniosku o zawarcie umowy faktoringu (art. 26 ust. 1 pkt 4 ustawy);
7) niezawarciu w umowie powierzenia przetwarzania danych, o której mowa w art. 31 ustawy, tj. w umowie z dnia […] lutego 2007 r. zawartej z O. Sp. z o.o., zakresu i celu przetwarzania danych powierzonych przez Spółkę ww. pomiotowi w związku z korzystaniem z systemu informatycznego o nazwie „B" (art. 31 ust. 1 i ust. 2 ustawy);
8) niezawarciu w umowie powierzenia przetwarzania danych, o której mowa w art. 31 ustawy, tj. w umowie z dnia […] czerwca 2006 r. na udzielenie sublicencji na system informatyczny „A" oraz w umowie współpracy z dnia […] maja 2003 r. zawartej z BZ. S.A., zakresu i celu przetwarzania danych powierzonych przez Spółkę, w związku z korzystaniem z systemu informatycznego o nazwie „C", służącego do przetwarzania danych osobowych osób reprezentujących klientów Spółki oraz danych poręczycieli, oraz z systemu informatycznego o nazwie „A", służącego do przetwarzania danych osobowych osób dokonujących transakcji (art. 31 ust. 1 i ust. 2 ustawy);
9) braku w polityce bezpieczeństwa informacji, o których mowa § 4 pkt 1, pkt 2, pkt 3 i pkt 4 rozporządzenia, tj.: 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; sposobu przepływu danych pomiędzy poszczególnymi systemami;
10) braku w instrukcji zarządzania systemem informatycznym informacji, o których mowa § 5 pkt 1, pkt 2, pkt 3, pkt 4, pkt 5, pkt 7 i pkt 8 rozporządzenia, tj. procedurach nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności; stosowanych metodach i środkach uwierzytelnienia oraz procedurach związanych z ich zarządzaniem i użytkowaniem; procedurach rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu; procedurach tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; sposobie, miejscu i okresie przechowywania: a) elektronicznych nośników informacji zawierających dane osobowe, b) kopii zapasowych, o których mowa w pkt 4; sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;

procedurach wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;

11) niezapewnieniu przez system informatyczny o nazwie „D" odnotowania identyfikatora użytkownika wprowadzającego dane osobowe do systemu; odnotowanie ww. informacji następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych (art. 38 ustawy, § 7 ust. 1 pkt 2 i ust. 2 rozporządzenia);
12) niezapewnieniu przez system informatyczny o nazwie „D", służący do przetwarzania danych osób reprezentujących klientów B. Sp. z o.o., sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu (art. 38 ustawy, § 7 ust. 3 rozporządzenia);
13) nienadaniu osobom dopuszczonym do przetwarzania danych osobowych upoważnienia do ich przetwarzania (art. 37 ustawy);
14) nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych (art. 39 ust. 1 ustawy);
15) niedokonaniu aktualizacji zbioru danych o nazwie „K" w zakresie zgłoszenia zmian co do wskazania aktualnego adresu swojej siedziby, opisu kategorii osób których dane dotyczą (tj. poręczycieli), zakresu danych poręczycieli oraz podstawy prawnej ich przetwarzania (art. 41 ust. 2 ustawy).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne sygn. […], w celu wyjaśnienia okoliczności sprawy.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes Zarządu Spółki pismami z dnia […] stycznia 2012 r. oraz z dnia […] marca 2012 r. złożył wyjaśnienia, w których poinformował m.in., że:

1. Spółka wprowadziła formularz o nazwie „Karta Identyfikacyjna" wypełniany przez osoby reprezentujące klienta w trakcie składania wniosku faktoringowego.
2. Spółka zaprzestała pozyskiwania zgody od osób reprezentujących podmioty gospodarcze na przetwarzanie ich danych osobowych dla celów związanych z działalnością Spółki.
3. W „Karcie Identyfikacyjnej" zamieszczono klauzulę o treści: *„Wyrażam/nie wyrażam zgodę na udostępnienie przez Spółki […] na rzecz B. Sp. z o.o. wszelkich informacji posiadanych na mój temat, w tym również objętych tajemnicą bankową w celu rozpatrzenia wniosku faktoringowego, oceny zdolności faktoringowej, analizy ryzyka faktoringowego i zawarcia umowy faktoringowej"*.

4. W „Karcie Identyfikacyjnej" zamieszczono klauzulę o treści: *„W celu tworzenia lub kierowania do mnie oferty produktowej upoważniam/ nie upoważniam Spółki […] oraz Fundusz […]i inny fundusz utworzony w przyszłości, którego organem jest B. Towarzystwo […] do wzajemnego przekazywania lub otrzymywania pomiędzy Spółkami/ Funduszami a także do przetwarzania przez każdą Spółkę/Fundusz mich danych osobowych lub danych stanowiących tajemnicę bankową lub tajemnicę zawodową lub danych stanowiących tajemnicę dotyczącą ubezpieczenia („Dane"), a w szczególności: danych identyfikacyjnych (w tym danych teleadresowych, adresu poczty elektronicznej, numeru PESEL, NIP, numeru paszportu i numeru dowodu osobistego); informacji o umowach zawartych z tą Spółką/Funduszem, w tym w szczególności o ich zakresie i sposobie zawarcia; informacji o stanie moich rachunków, pobranych opłatach, oraz transakcjach dokonanych w związku z umowami zawartymi z tą Spółką/Funduszem, w szczególności danych zawartych w rejestrach uczestników tego Funduszu oraz danych powstałych w skutek przetwarzania danych wskazanych powyżej; z zastrzeżeniem, że Dane takie przekazywane będą wielokrotnie, na bieżąco, w celu uwzględnienia zmian Danych. Zgoda ta obejmuje również przetwarzanie tych danych w przyszłości, jeżeli nie zmieni się cel przetwarzania"*.
5. Spółka określiła podmioty, którym dane będą udostępniane oraz podmioty, od jakich dane będą pozyskiwane, poprzez wyszczególnienie członków Grupy Kapitałowej […].
6. Spółka w „Karcie identyfikacyjnej" zamieściła informację o celu udostępniania danych podmiotom należącym do Grupy Kapitałowej […] (tj. w celu tworzenia lub kierowania pełnej oferty produktowej) oraz informację o celu pozyskiwania danych od podmiotów Grupy Kapitałowej […] (tj. w celu rozpatrzenia wniosku faktoringowego, oceny zdolności faktoringowej, analizy ryzyka faktoringowego i zawarcia umowy faktoringowej, a także w celu tworzenia lub kierowania pełnej oferty produktowej).
7. Spółka zamieściła informację o celach przetwarzania danych, tj. celu rozpatrzenia wniosku faktoringowego, oceny zdolności faktoringowej, analizy ryzyka faktoringowego, zawarcia i realizacji umowy faktoringowej, w celach identyfikacyjnych, w celu tworzenia i kierowania pełnej oferty produktowej oraz w celu realizacji przepisów ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. nr 46, poz. 276 ze zm.), a także informację o podstawie prawnej obowiązku podania danych.
8. Spółka będzie pozyskiwać od potencjanych klientów oraz poręczycieli weksli dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez Spółkę przetwarzane. Spółka nie będzie zbierała i przetrzymywała kopii dowodów osobistych. W celu

zbierania i przetwarzania danych wprowadzono Kartę Identyfikacyjną. Spółka będzie zbierała, przechowywała i przetwarzała dane w zakresie: imię, nazwisko, data urodzenia, numer i seria dowodu osobistego, adres zamieszkania, adres korespondencyjny, dane kontaktowe (numer telefonu, adres e-mail), numer PESEL, obywatelstwo.

9. W przypadku gdy umowa faktoringowa nie zostanie podpisana, zgromadzone dane zostaną usunięte a przetwarzanie zakończone. System informatyczny o nazwie „C" został wycofany z eksploatacji i zostały z niego usunięte wszystkie dane osobowe. Wnioski o zawarcie umowy faktoringowej, które zostały rozpatrzone przez Spółkę negatywnie również zostały usunięte z ww. systemu.
10. Spółka przechowuje dane w postaci papierowej w archiwum O. Sp. z o.o. Przekazywane do archiwum dane są zabezpieczone i zaplombowane. Nie jest możliwy dostęp do przechowywanych danych osobowych osobom nieupoważnionym do ich przetwarzania. Dane osobowe przechowywane w ww. podmiocie nie podlegają skanowaniu przez O. Sp. z o.o.
11. Administratorem systemu informatycznego o nazwie „B" jest Bank S.A. w systemie tym zamieszczona jest dokumentacja dotycząca klientów Spółki w formie zdigitalizowanej. Korzystanie przez Spółkę z ww. systemu odbywa się na podstawie umowy z dnia [ ] marca 2008 r. na świadczenie usług archiwizacji danych zawartej z Bankiem S.A.
12. Spółka zobowiązała się do podpisania aneksu do umowy zawartej z Bankiem S.A. w celu skonkretyzowania zakresu oraz celu przetwarzania danych powierzonych ww. podmiotowi w zakresie korzystania z systemu informatycznego o nazwie „A".
13. Spółka znowelizowała procedurę dotyczącą ochrony danych osobowych, poprzez wprowadzenie załączników: wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych.
14. Zaktualizowano procedurę zakładania nowych użytkowników oraz nadawania/zmiany/cofania uprawnień użytkownikom systemów informatycznych Spółki.
15. Stosowane metody i środki uwierzytelniania w systemach zostały opisane w podręczniku „Bezpieczeństwo informacji w […].
16. Harmonogram tworzenia oraz przechowywania kopii zapasowych systemów zarządzanych przez Spółkę jest elementem załącznika nr […] do umowy […] zawartej z Bankiem S.A., która reguluje kwestie dotyczące tworzenia kopii zapasowych wszystkich serwerów Spółki.
17. Kwestie związane z przeglądem oraz konserwacją systemów są procesowane zgodnie z „Procedurą zarządzania incydentami, zmianami oraz wgrywaniem poprawek dot. systemów informatycznych […]".

18. Pracownikom Spółki, którzy posiadają dostęp do danych osobowych zostały nadane upoważnienia do przetwarzania danych osobowych.
19. System informatyczny o nazwie „D” zapewnia odnotowanie informacji o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu. Odnotowanie identyfikatora użytkownika w systemie następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
20. System informatyczny o nazwie „D” zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o identyfikatorze użytkownika wprowadzającego dane do systemu.
21. Spółka prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
22. Spółka dokonała aktualizacji zbioru danych o nazwie „K” w zakresie wskazania aktualnego adresu swojej siedziby, opisu kategorii osób, których dane dotyczą, tj. poręczycieli, wskazania zakresu danych poręczycieli jaki jest przetwarzany oraz podstawy prawnej ich przetwarzania.

Ponadto, do ww. pism załączono: kopię uchwały Zarządu B. Sp. z o.o. nr […] z dnia […] stycznia 2012 r. w sprawie wprowadzenia do stosowania w B. Sp. z o.o. Karty Identyfikacyjnej wraz z wzorem ww. karty; kopię uchwały Zarządu B. Sp. z o.o. nr […] z dnia […] marca 2012 r. w sprawie wprowadzenia do stosowania w B. Sp. z o.o. nowego wzoru Karty Identyfikacyjnej wraz z wzorem ww. karty; kopię zarządzenia Prezesa Zarządu nr […] z dnia […] stycznia 2012 r. w sprawie wprowadzenia zmian we wzorach dokumentów faktoringowych w B. Sp. z o.o. wraz z wzorem wniosku o przyznanie limitu faktoringowego/limitu na finansowanie dostaw; kopię uchwały Zarządu B. Sp. z o.o. nr […] z dnia […] stycznia 2012 r. w sprawie wprowadzenia zasad ochrony danych osobowych w B. Sp. z o.o. wraz z kopią ww. dokumentu i załącznikami nr 1 i nr 2; kopię pakietu prac nr 1 - udzielenie licencji wdrożenia systemu „A” z dnia […] czerwca 2003 r.; kopię dokumentu o nazwie „Analiza systemu […]”; wydruk Podręcznika Bezpieczeństwa Informacji TOM […]; kopię umowy nr […] na świadczenie usług IT z dnia […] lipca 2009 r. zawartej z BZ S.A. wraz z załącznikami; kopię uchwały Zarządu B. Sp. z o.o. nr […] z dnia […] stycznia 2012 r. w sprawie wprowadzenia procedury zarządzania incydentami, zmianami oraz wgrywaniem poprawek dot. systemów informatycznych w B. Sp. z o.o. wraz z kopią ww. procedury; kopię specyfikacji do raportu dot. zmian związanych z EBI Faktor; zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych o nazwie „K; kopię uchwały Zarządu B. Sp. z o.o. nr […] z dnia […] stycznia 2012 r. w sprawie wprowadzenia nowej procedury zakładania użytkownikom oraz nadawania/zmiany/cofania uprawnień użytkownikom w

systemach informatycznych BZ. w B. Sp. z o.o. wraz z kopią ww. procedury; kopię ewidencji osób upoważnionych do przetwarzania danych osobowych w BZ.; kopię umowy z dnia […] marca 2008 r. o świadczenie usług archiwizacji danych zawartą z Bankiem S.A. wraz z aneksem nr 1.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie, Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje:

Zgodnie z art. 31 ust. 1 i ust. 2 ustawy administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

W toku kontroli ustalono, iż rejestr, o którym mowa w art. 8 ust. 1 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r., Nr 46, poz. 276 z późn. zm.) prowadzony jest wyłącznie w systemie informatycznym o nazwie „A" i służy do udostępniania informacji z rejestru do Generalnego Inspektora Informacji Finansowej. Dane z rejestru są przechowywane na serwerach BZ. S.A. W zakresie przechowywania danych zawartych w rejestrze (system informatyczny o nazwie „A") Spółka zawarła pisemne umowy m.in. na przechowywanie danych z BZ S.A., tj. umowę z dnia […] czerwca 2006 r. na udzielenie sublicencji na system informatyczny „A' oraz umowę współpracy z dnia […] maja 2003 r.

Z analizy ww. umów nie wynikało aby był w nich określony zakres i cel przetwarzania danych powierzonych BZ S.A., w związku z korzystaniem z systemu informatycznego o nazwie „A".

W toku postępowania Spółka zobowiązała się do podpisania aneksu do umowy zawartej z Bankiem S.A., tj. do umowy z dnia […] czerwca 2006 r. na udzielenie sublicencji na system informatyczny „A", konkretyzującego zakres oraz cel przetwarzania danych powierzonych przez Spółkę ww. podmiotowi, w zakresie korzystania z systemu informatycznego o nazwie „A".

W oparciu o powyższe wyjaśnienia nie można jednak uznać, iż w przedmiotowym zakresie został przywrócony stan zgodny z prawem. Z uwagi na powyższe, Generalny Inspektor nakazał administratorowi danych, tj. B. Sp. z o.o., określenie w umowie powierzenia przetwarzania danych zawartej z BZ S.A., dotyczącej korzystania z systemu informatycznego o nazwie „A" (służący do przetwarzania danych osobowych osób dokonujących transakcji), zakresu i celu powierzenia danych ww. osób, wyznaczając przy tym odpowiedni termin na usunięcie przedmiotowego uchybienia.

Zgodnie § 4 pkt 1, pkt 2, pkt 3 i pkt 4 rozporządzenia polityka bezpieczeństwa powinna zawierać: 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym

przetwarzane są dane osobowe; 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; 4) sposób przepływu danych pomiędzy poszczególnymi systemami.

W toku kontroli ustalono, iż w posiadanej przez Spółkę polityce bezpieczeństwa brak jest: 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 dla systemów informatycznych o nazwach „C" i „A"; sposobu przepływu danych pomiędzy poszczególnymi systemami.

W toku postępowania Spółka wyjaśniła, iż system informatyczny o nazwie „C" został wycofany z eksploatacji i zostały z niego usunięte wszystkie dane osobowe. Ponadto, Spółka znowelizowała procedurę dotyczącą ochrony danych osobowych, poprzez wprowadzenie załączników: wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe, oraz wykaz zbiorów danych osobowych.

Z analizy załączników do ww. procedury wynika, iż załącznik nr 1 do procedury ochrony danych osobowych o nazwie „Wykaz budynków, pomieszczeń w których przetwarzane są dane osobowe" nie zawiera wykazu pomieszczeń, w których przetwarzane są dane osobowe. Ponadto z analizy załącznika nr […] o nazwie „Wykaz zbiorów danych osobowych" do ww. procedury wynika, iż nie zawiera on informacji dotyczących systemu informatycznego o nazwie „A", który służy do przetwarzania danych osobowych osób dokonujących transakcji. Jednocześnie w polityce bezpieczeństwa brak jest informacji w zakresie opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami.

Zgodnie z § 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.

W toku kontroli ustalono, iż system informatyczny o nazwie „D" dla każdej osoby, której dane osobowe są przetwarzane w ww. systemie informatycznym nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu.

W toku postępowania Spółka wyjaśniła, iż dokonała modyfikacji systemu informatycznego o nazwie „D", który zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu. Na potwierdzenie ww. wyjaśnień Spółka przesłała przykładowy raport z ww. informacjami.

Z analizy przedmiotowego raportu wynika jednak, iż zastosowano kryterium wyszukiwania według daty początkowej i końcowej, a nie kryterium wyszukiwania według danych osobowych np.: imienia, nazwiska, numeru pesel. Zatem uznać należy, iż system informatyczny o nazwie „D" **dla każdej osoby**, której dane osobowe są przetwarzane w ww. systemie informatycznym nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu.

W świetle złożonych przez Spółkę wyjaśnień oraz pozostałych dowodów uznać należy, iż w toku postępowania usunięte zostały uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania poprzez:

1) zapewnienie osobom reprezentującym podmioty gospodarcze, będące klientami B. Sp. z o.o., swobody wyrażenia zgody na udostępnienie danych przez B. Sp. z o.o. podmiotom należącym do Grupy Kapitałowej Banku […], swobody wyrażenia zgody na udostępnienie danych przez podmioty Grupy Kapitałowej Banku […] na rzecz B. Sp. z o.o.;
2) zaprzestanie pozyskiwania zgody od osób reprezentujących podmioty gospodarcze na przetwarzanie ich danych osobowych dla celów związanych z działalnością Spółki;
3) zamieszczenie w „Karcie identyfikacyjnej" informacji o celu udostępniania danych podmiotom należącym do Grupy Kapitałowej Banku […] (tj. w celu tworzenia i kierowania pełnej oferty produktowej) oraz informację o celu pozyskiwania danych od podmiotów Grupy Kapitałowej Banku […] (tj. w celu rozpatrzenia wniosku faktoringowego, oceny zdolności faktoringowej, analizy ryzyka faktoringowego i zawarcia umowy faktoringowej, a także w celu tworzenia i kierowania pełnej oferty produktowej);
4) dopełnianie obowiązku informacyjnego wobec osób reprezentujących podmioty gospodarcze, będące klientami B. Sp. z o.o., w zakresie informowania o celu przetwarzania danych, tj. w celu rozpatrzenia wniosku i zawarcia umowy faktoringu oraz o podstawie prawnej pozyskiwania danych, tj. ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. nr 46, poz. 276 ze zm.);

5) zaprzestanie pozyskiwania od osób reprezentujących podmioty gospodarcze, będące klientami B. Sp. z o.o., danych w zakresie: nazwiska rodowego, imion rodziców, miejsca urodzenia, płci, wzrostu, koloru oczu, wizerunku;
6) zaprzestanie pozyskiwania od poręczycieli klientów danych w zakresie: nazwiska rodowego, imion rodziców, miejsca urodzenia, płci, wzrostu, koloru oczu, wizerunku;
7) zapewnienie, że dane osób reprezentujących podmioty gospodarcze, będące klientami B. Sp. z o.o., oraz poręczycieli klientów będą przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, w przypadku gdy umowa nie zostanie zawarta, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, tj. rozpatrzenia wniosku o zawarcie umowy faktoringu;
8) wycofanie systemu informatycznego o nazwie „C" z eksploatacji i usunięcie z niego wszystkich danych osobowych;
9) wyjaśnienie, iż dane osobowe przechowywane w O. Sp. z o.o. nie podlegają skanowaniu, oraz iż administratorem systemu informatycznego o nazwie „B" jest Bank […], oraz że w systemie tym zamieszczona jest dokumentacja dotycząca klientów Spółki w formie zdigitalizowanej. Korzystanie przez Spółkę z ww. systemu odbywa się na podstawie umowy z dnia […] marca 2008 r. na świadczenie usług archiwizacji danych zawartej z Bankiem […];
10) uzupełnienie instrukcji zarządzania systemem informatycznym o informacje, o których mowa § 5 pkt 1, pkt 2, pkt 3, pkt 4, pkt 5, pkt 7 i pkt 8 rozporządzenia tj.: procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; sposób, miejsce i okres przechowywania: a) elektronicznych nośników informacji zawierających dane osobowe, b) kopii zapasowych, o których mowa w pkt 4; sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4; procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
11) zapewnienie, aby system informatyczny o nazwie „D" odnotowywał identyfikator użytkownika wprowadzającego dane osobowe do systemu;

12) zapewnienie, aby system informatyczny o nazwie „D” odnotowywał identyfikator użytkownika wprowadzającego dane osobowe do systemu, automatycznie po zatwierdzeniu przez użytkownika opcji wprowadzania danych;
13) nadanie osobom dopuszczonym do przetwarzania danych osobowych upoważnienia do ich przetwarzania;
14) prowadzenie ewidencji osób upoważnionych do przetwarzania danych;
15) dokonanie aktualizacji zbioru danych o nazwie „K” w zakresie zgłoszenia zmian co do wskazania aktualnego adresu swojej siedziby, opisu kategorii osób których dane dotyczą (tj. poręczycieli), zakresu danych poręczycieli oraz podstawy prawy prawnej ich przetwarzania.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe w całości albo w części, organ administracji publicznej wydaje decyzję o umorzeniu postępowania odpowiednio w całości albo w części. Przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a. jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny”, czyli każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. S.A./Sz 1029/97).

Z uwagi na to, iż usunięte zostały pozostałe uchybienia będące przedmiotem niniejszego postępowania administracyjnego, postępowanie należało w tym zakresie umorzyć.

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

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.