



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 25 stycznia 2010 r.

DIS/DEC-93/3187/10

dot. [...]

D E C Y Z J A

Na podstawie art. 105 § 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 i art. 22 w związku z art. 26 ust. 1 pkt 1 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 3 i pkt 4, § 5 pkt 6, § 7 ust. 1 pkt 1 i pkt 2 oraz § 7 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 „P” Sp. z o.o.,

umarzam postępowanie w niniejszej sprawie.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili w „P” Sp. z o.o, zwaną dalej również Spółką, kontrolę 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 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), zwanym dalej również

rozporządzeniem. W toku kontroli odebrano od pracowników Spółki ustne wyjaśnienia 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. Przetwarzaniu z naruszeniem przepisów prawa, danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Spółki w celu ewidencji czasu pracy (art. 26 ust. 1 pkt 1 ustawy).
2. Nieuwzględnieniu w polityce bezpieczeństwa opisu struktury zbiorów danych, wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 3 i pkt 4 rozporządzenia).
3. Nieuwzględnieniu w instrukcji zarządzania systemem informatycznym sposobu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w części A pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia).
4. Niezapewnieniu, aby system informatyczny o nazwie „A”, w którym są przetwarzane dane osobowe pracowników Spółki, zapewniał dla każdej osoby, której dane są przetwarzane w systemie, odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu (§ 7 ust. 1 pkt 2 rozporządzenia).
5. Niezapewnieniu, aby system informatyczny o nazwie „B”, w którym są przetwarzane dane osobowe pracowników Spółki, zapewniał dla każdej osoby, której dane są przetwarzane w systemie, odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu (§ 7 ust. 1 pkt 1 i pkt 2 rozporządzenia).
6. Niezapewnieniu, aby w raporcie oferowanym przez system informatyczny o nazwie „A” był uwzględniony identyfikator użytkownika wprowadzającego dane do systemu, ponadto, niezapewnieniu przez system informatyczny o nazwie „B” sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane do systemu (§ 7 ust. 3 rozporządzenia).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności

sprawy. Pismem zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie [...], administrator danych został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, Pełnomocnik Spółki (pełnomocnictwo w aktach sprawy), w piśmie z dnia [...] listopada 2009 r., złożył wyjaśnienia, w których poinformował m.in., że:

1. Zarządzeniem Prezesa Zarządu Spółki z dnia [...] listopada 2009 r. odstąpiono od stosowania systemu potwierdzania czasu pracy za pomocą odcisku linii papilarnych, likwidując czytnik linii papilarnych. Dane biometryczne zostały usunięte z czytnika, pliki backupów zostały skasowane komisyjnie, natomiast program do zarządzania czytnikiem odinstalowano. Wykonanie powyższych czynności zostało potwierdzone protokołem usunięcia danych biometrycznych pracowników P. Sp. z o.o. Obecnie pracownicy Spółki rejestrują czas pracy logując się czterocyfrowym pinem.
2. Z uwagi na stwierdzenie, iż w polityce bezpieczeństwa nie uwzględniono opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, została opracowana dokumentacja, w której zawarto opis „tabeli przechowującej dane osobowe”, udokumentowano również powiązanie aplikacji „B” z systemem kadrowym „A”. Dokumentacja ta zostanie dołączona do „Polityki bezpieczeństwa”.
3. „Polityka bezpieczeństwa” zostanie uzupełniona o punkt „Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego”.
4. W systemie „A” została włączona opcja pozwalająca na wygenerowanie raportu o tym, jaki użytkownik i kiedy zmieniał dane osobowe.
5. W systemie „B” został utworzony raport, który umożliwia podgląd daty utworzenia i modyfikacji danych użytkownika oraz określa, który użytkownik dokonał rejestracji bądź modyfikacji.

Do ww. pisma zostały załączone, pozostałe dowody mające potwierdzić przesłane wyjaśnienia: kopia protokołu usunięcia danych biometrycznych pracowników Spółki, opis powiązania systemu „B” z innymi systemami, zrzut ekranu aplikacji „A” raport wprowadzania i modyfikacji danych użytkowników w aplikacji „B”. Ponadto, w dniu [...] grudnia 2009 r. do Biura GIODO wpłynęło pismo Pełnomocnika Spółki, do którego załączono kopię dokumentu o nazwie „Procedura eksploatacji systemów informatycznych. Polityka bezpieczeństwa. Instrukcja zarządzania systemem informatycznym do przetwarzania danych osobowych”.

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

Na podstawie złożonych przez Pełnomocnika Spółki wyjaśnień i pozostałych załączonych dowodów należy stwierdzić, że uchybienia w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania zostały usunięte, tj.:

1. Spółka zaprzestała przetwarzania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Spółki w celu ewidencji czasu pracy.
2. W dokumencie o nazwie „Procedura eksploatacji systemów informatycznych. Polityka bezpieczeństwa. Instrukcja zarządzania systemem informatycznym do przetwarzania danych osobowych” uwzględniono opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.
3. W dokumencie o nazwie „Procedura eksploatacji systemów informatycznych. Polityka bezpieczeństwa. Instrukcja zarządzania systemem informatycznym do przetwarzania danych osobowych” uwzględniono sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w części A pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia).
4. Zapewniono, aby system informatyczny o nazwie „A”, w którym są przetwarzane dane osobowe pracowników Spółki odnotowywał identyfikator użytkownika wprowadzającego dane do systemu.
5. Zapewniono, aby system informatyczny o nazwie „B”, w którym są przetwarzane dane osobowe pracowników Spółki odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane do systemu.
6. Zapewniono, aby w raporcie oferowanym przez system informatyczny o nazwie „A” był uwzględniony identyfikator użytkownika wprowadzającego dane do systemu.
7. Zapewniono, aby system informatyczny o nazwie „B” zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane do systemu (§ 7 ust. 3 rozporządzenia).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a jest bezprzedmiotowość postępowania „z jakiegokolwiek przyczyny”, czyli z 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. SA/Sz1029/97).

W toku postępowania usunięte zostały uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego należało je umorzyć.

Wobec powyższego, 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.