



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 18 lutego 2011 r.

DIS/DEC-119/7194/11

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 (Dz. U. z 2000 r., Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 26 ust. 1 pkt 4, art. 36 ust. 1 i ust. 2, art. 38 oraz art. 39 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), a także § 4 pkt 3, § 7 ust. 1 pkt 1 i pkt 2, § 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) oraz częścią A pkt II ust. 1, częścią A pkt II ust. 2 lit. a i lit. b, częścią A pkt IV ust. 2, częścią A pkt V, częścią B pkt VIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Zespół Szkół Rolniczych,

I. Nakazuję Zespołowi Szkół Rolniczych, jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

- 1. Stosowanie mechanizmów kontroli dostępu do danych osobowych czytelników przetwarzanych w systemie informatycznym o nazwie „A”, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Zapewnienie, aby w systemie informatycznym o nazwie „B”, w którym przetwarzane są dane osobowe pracowników oraz w systemie informatycznym o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, dla każdego użytkownika ww. systemów rejestrowany był odrębny identyfikator, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

3. Zapewnienie, aby dostęp do danych osobowych czytelników przetwarzanych w systemie informatycznym o nazwie „A” był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.
4. Zapewnienie, aby hasło dostępu do systemu informatycznego o nazwie „B”, w którym przetwarzane są dane osobowe pracowników, było zmieniane nie rzadziej, niż co 30 dni, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.
5. Stosowanie środków ochrony kryptograficznej wobec danych osobowych pracowników przetwarzanych za pomocą systemu informatycznego o nazwie „C” na komputerze przenośnym użytkowanym przez Wicedyrektora Zespołu Szkół, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.
6. Uzupełnienie polityki bezpieczeństwa, prowadzonej w postaci dokumentu o nazwie „Dokumentacja Systemu [...]”, o opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
7. Zapewnienie, aby system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, odnotowywał datę pierwszego wprowadzenia danych oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.
8. Zapewnienie, aby systemy informatyczne o nazwach: „B”, „D” oraz „E”, wykorzystywane do przetwarzania danych osobowych pracowników, zapewniały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 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), w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w Zespole Szkół Rolniczych, zwanym dalej również ZSR, w celu ustalenia

zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. akt [...], 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. W toku kontroli m.in. odebrano od pracowników ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli sygn. [...], który został podpisany przez Dyrektora ZSR. Na podstawie całokształtu materiału dowodowego zgromadzonego w sprawie ustalono, że Zespół Szkół Rolniczych, jako administrator danych, naruszył przepisy o ochronie danych osobowych. Stwierdzone uchybienia polegały na:

1. Przechowywaniu danych osobowych kandydatów nieprzyjętych do szkół dziennych dla młodzieży wchodzących w skład ZSR, w postaci umożliwiającej identyfikację osób, których dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 4 ustawy).
2. Niestosowaniu mechanizmów kontroli dostępu do danych osobowych czytelników przetwarzanych w systemie informatycznym o nazwie „A” (część A pkt II ust. 1 załącznika do rozporządzenia).
3. Niezapewnieniu, aby w systemie informatycznym o nazwie „B”, w którym przetwarzane są dane osobowe pracowników oraz w systemie informatycznym o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, dla każdego użytkownika ww. systemów rejestrowany był odrębny identyfikator (część A pkt II ust. 2 lit. a załącznika do rozporządzenia).
4. Niezapewnieniu, aby dostęp do danych osobowych czytelników przetwarzanych w systemie informatycznym o nazwie „A” był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia (część A pkt II ust. 2 lit. b załącznika do rozporządzenia).
5. Niezapewnieniu, aby hasło dostępu do systemu informatycznego o nazwie „B”, w którym przetwarzane są dane osobowe pracowników, było zmieniane nie rzadziej, niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
6. Niestosowaniu środków ochrony kryptograficznej wobec danych osobowych pracowników przetwarzanych za pomocą systemu informatycznego o nazwie „C” na komputerze przenośnym użytkowanym przez Wicedyrektora Zespołu Szkół Rolniczych (część A pkt V załącznika do rozporządzenia).

7. Niezapewnieniu, aby hasło do systemu informatycznego o nazwie „B”, w którym przetwarzane są dane osobowe pracowników, zainstalowanego na stacji roboczej połączonej z siecią publiczną, składało się z co najmniej z 8 znaków (część B pkt VIII załącznika do rozporządzenia).

8. Niezawarciu w polityce bezpieczeństwa prowadzonej w postaci dokumentu o nazwie „Dokumentacja Systemu [...]” (§ 4 pkt 3 rozporządzenia).

9. Niezapewnieniu, aby system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, odnotowywał datę pierwszego wprowadzenia danych oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 1 i pkt 2 rozporządzenia).

11. Niezapewnieniu, aby systemy informatyczne o nazwach: „B”, „D” oraz „E”, wykorzystywane do przetwarzania danych osobowych pracowników, zapewniały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 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) - § 7 ust. 3 rozporządzenia.

11. Niewskazaniu w ewidencji osób upoważnionych do przetwarzania danych identyfikatora, osoby upoważnionej do przetwarzania danych w systemie informatycznym (art. 39 ust. 1 pkt 3 ustawy).

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 nr [...], 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 pismem z dnia [...] stycznia 2011 r. administrator danych przesłał wyjaśnienia w sprawie stwierdzonych uchybień, z których wynika że:

1. Dokumenty rekrutacyjne uczniów nieprzyjętych do Szkół prowadzonych przez ZSR zostały komisyjnie zniszczone w dniu [...] grudnia 2010 r.

2. W dniu [...] stycznia 2011 r. przeprowadzono migrację danych przetwarzanych w systemie informatycznym o nazwie „A” do jego nowej wersji, tj. systemu informatycznego „A”. W ramach jego konfiguracji dokonano włączenia pracy wielodostępu w systemie informatycznym „A” oraz utworzono indywidualne konta dostępu dla użytkowników ww. systemu. Ponadto uruchomiono mechanizm automatycznego wymuszenia zmiany hasła użytkownika po upływie 30 dni. Zainstalowanie nowej wersji

systemu informatycznego o nazwie „A” skutkowało również usunięciem uchybienia dotyczącego niezapewnienia odnotowywania daty pierwszego wprowadzenia danych oraz identyfikatora użytkownika wprowadzającego dane osobowe czytelników do tego systemu. Aktualnie użytkowana wersja systemu informatycznego o nazwie „A” zapewnia zidentyfikowanie użytkownika, który wprowadził do systemu określony rekord.

3. W miesiącu listopadzie 2010 r. rozdzielono funkcję administratora oprogramowania oraz użytkownika systemu informatycznego o nazwie „B”, wykonującego bieżącą pracę w programie. Hasło dostępu użytkownika do ww. systemu informatycznego zostało zmienione na 8 znakowe. Zmiana hasła dostępu do systemu informatycznego o nazwie „B” jest wymuszana automatycznie przez ten system informatyczny. Powodem, dla którego użytkownik ww. systemu informatycznego wyjaśnił w toku kontroli, iż hasło do systemu informatycznego o nazwie „B” nie jest zmieniane, była sytuacja, iż w tym czasie nie upłynął jeszcze okres 30 dni od dnia, w którym zainstalowano ww. system na stacji roboczej i przypisano użytkownikowi indywidualne hasło dostępu.

4. Rozszerzono ewidencję osób upoważnionych do przetwarzania danych osobowych o identyfikator osoby upoważnionej, w przypadku przetwarzania przez nią danych osobowych w systemie informatycznym.

Na potwierdzenie powyższych wyjaśnień do powołanego pisma załączono uwierzytelnione kopie „Protokołu oceny dokumentacji niearchiwalnej”, „Spisu dokumentacji przeznaczonej do zniszczenia” oraz „Ewidencji osób upoważnionych do przetwarzania danych w systemach informatycznych”.

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

Zgodnie z 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.

Zgodnie z częścią A pkt II ust. 1 załącznika do rozporządzenia, w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „A” służącym do obsługi biblioteki ZSR, w którym przetwarzane są dane osobowe czytelników, nie są stosowane mechanizmy kontroli dostępu do danych. Pismem z dnia [...] listopada 2010 r. administrator danych

wyjaśnił, iż w miarę posiadanych środków finansowych przygotowana zostanie procedura migracji ww. systemu do jego nowszej wersji zgodnej z wymogami ustawy. Kolejnym pismem z dnia [...] stycznia 2011 r. administrator danych poinformował, iż od dnia [...] stycznia 2011 r. dane osobowe czytelników przetwarzane są w ZSR za pomocą nowej wersji systemu informatycznego „A” a także, iż dla użytkowników ww. systemu informatycznego utworzono indywidualne konta dostępu do danych. W tym miejscu należy jednak zauważyć, iż w toku niniejszego postępowania ZSR nie wykazał w sposób dostateczny, iż powyższe wyjaśnienia są zgodne z aktualnym stanem faktycznym. Przedstawiona kopia „Ewidencji osób upoważnionych do przetwarzania danych w systemach informatycznych”, w której m.in. wskazano identyfikatory (loginy) użytkowników systemu informatycznego o nazwie „A”, nie stanowi bowiem w tym przypadku wystarczającego dowodu na potwierdzenie złożonych wyjaśnień. Dowód taki mógłby natomiast stanowić np. wydruk z systemu informatycznego o nazwie „A”, przedstawiający rejestr jego użytkowników wraz z „zrzutem ekranu” z ww. systemu przedstawiającym okno logowania użytkownika. Mając powyższe na uwadze należy stwierdzić, iż przedstawione przez ZSR dowody na usunięcie ww. uchybienia, w postaci pisemnych wyjaśnień administratora danych oraz kopii „Ewidencji osób upoważnionych do przetwarzania danych w systemach informatycznych”, nie stanowią wystarczającej podstawy do uznania, że w ww. zakresie został przywrócony stan zgodny z prawem.

Zgodnie z częścią A pkt II ust. 2 lit. a, załącznika do rozporządzenia, jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają, co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.

W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „B”, w którym przetwarzane są dane osobowe pracowników ZSR, dla dwóch użytkowników ww. systemu stosowany jest jeden identyfikator. Ponadto ustalono, że w systemie informatycznym o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, dla czterech użytkowników ww. systemu stosowany jest jeden identyfikator.

W toku niniejszego postępowania administrator danych nie przedstawił dowodów (np. wydruków z ww. systemów informatycznych przedstawiających rejestry ich użytkowników), na podstawie których możliwym było by uznanie, iż ww. uchybienia zostały usunięte. Za dowód taki nie można bowiem uznać kopii „Ewidencji osób upoważnionych do przetwarzania danych w systemach informatycznych”.

Zgodnie z częścią A pkt II ust. 2 lit. b, załącznika do rozporządzenia, jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają, co najmniej dwie osoby, wówczas zapewnia się, aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

W toku czynności kontrolnych ustalono, że dostęp do danych przetwarzanych w systemie informatycznym o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, nie wymaga uwierzytelnienia użytkownika. Pismem z dnia [...] stycznia 2011 r. ZSR wyjaśnił, iż w obecnie użytkowanej wersji systemu informatycznego o nazwie „A” utworzono indywidualne konta dostępu do danych dla użytkowników ww. systemu. Na potwierdzenie wyżej wskazanych wyjaśnień nie przedstawiono jednak innych dowodów (np. wydruków z systemu informatycznego o nazwie „A”, przedstawiających rejestr jego użytkowników wraz z „zrzutem ekranu” z ww. systemu przedstawiającym okno logowania użytkownika), które pozwalały by stwierdzić, iż odzwierciedlają one aktualny stan faktyczny. Powyższe wyjaśnienia administratora danych nie stanowią natomiast wystarczającej podstawy, aby możliwym było uznanie, iż w zakresie ww. uchybienia został przywrócony stan zgodny z prawem.

Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni. Hasło składa się, co najmniej z 6 znaków.

W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „B”, w którym przetwarzane są dane osobowe pracowników ZSR, nie jest zmieniane hasło dostępu. Z wyjaśnień złożonych przez administratora danych pismem z dnia [...] stycznia 2011 r. wynika natomiast, że zmiana hasła użytkownika w systemie informatycznym o nazwie „B” jest wymuszana co 30 dni przez ten system. Uzupełniając powyższe wyjaśnienia w powołanym piśmie wskazano, iż w toku kontroli użytkownik ww. systemu informatycznego wyjaśnił, że: *„hasło do B nie jest zmieniane”*, jedynie dlatego, gdyż w tym czasie nie upłynął jeszcze okres 30 dni od dnia, w którym opisywany system informatyczny zainstalowano na stacji roboczej i przypisano ww. użytkownikowi indywidualne hasło dostępu. Z uwagi na powyższe system informatyczny o nazwie „B” nie wymusił jeszcze w tym czasie zmiany hasła dostępu przez tego użytkownika.

Odnosząc się do powyższych wyjaśnień administratora danych trzeba jednak zauważyć, iż nie zostały one potwierdzone żadnymi innymi dowodami (np. wydrukiem „zrzutu ekranu” monitora z ustawieniami domenowej polityki bezpieczeństwa dotyczącej polityki haseł zawierającym takie dane jak: maksymalny okres żywotności hasła w dniach, minimalny okres ważności hasła w dniach). Mając powyższe na uwadze należy stwierdzić, iż ZSR nie udowodnił w sposób wystarczający, iż w przypadku systemu informatycznego o nazwie „B”, w którym przetwarzane są dane osobowe pracowników, wskazane powyżej przepisy o ochronie danych osobowych nie są naruszane.

Zgodnie z częścią A pkt V załącznika do rozporządzenia, osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność 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.

W toku czynności kontrolnych ustalono, że na komputerze przenośnym użytkowanym przez Wicedyrektora ZSR odbywa się przetwarzanie danych osobowych pracowników w systemie informatycznym o nazwie „C”. Jednocześnie ustalono, iż nie zastosowano środków ochrony kryptograficznej wobec danych przetwarzanych na ww. komputerze, a zatem w powyższym zakresie zostały naruszone obowiązujące przepisy prawa.

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją”. Jak stanowi § 4 pkt 3 rozporządzenia polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

W toku czynności kontrolnych ustalono, iż w ZSR prowadzona jest polityka bezpieczeństwa, o której mowa w § 3 ust. 1 rozporządzenia, w postaci dokumentu o nazwie „Dokumentacja Systemu [...]”. W wyniku analizy treści opisywanego dokumentu stwierdzono, iż brak jest w nim opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi, a zatem ww. dokument nie spełnia wymogu wskazanego w § 4 pkt 3 rozporządzenia.

Zgodnie z art. 38 ustawy administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Zgodnie z § 7 ust. 1 pkt 1 i pkt 2 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.

W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „A”, w którym przetwarzane są dane osobowe czytelników, możliwe jest automatyczne odnotowanie daty pierwszego wprowadzenia danych oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, lecz funkcjonalność ta nie jest wykorzystywana przez administratora danych. ZSR w toku niniejszego postępowania wyjaśnił, iż wdrożenie nowej wersji systemu informatycznego o nazwie „A” spowodowało

usunięcie powyższego uchybienia. Fakt ten nie został jednak potwierdzony żadnymi innymi dowodami (np. wydrukiem przykładowego rekordu, na którym oprócz danych osobowych wprowadzonych do systemu będzie widniała informacja o identyfikatorze użytkownika, który te dane wprowadził oraz dacie ich wprowadzenia). Dlatego też nie można uznać, iż wskazane powyżej uchybienie zostało usunięte.

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 czynności kontrolnych ustalono, że następujące systemy informatyczne służące do przetwarzania danych osobowych pracowników nie zapewniają sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1: 1) system informatyczny o nazwie „B”; 2) system informatyczny o nazwie „D”; 3) system informatyczny o nazwie „E”. W powyższym zakresie został zatem naruszony § 7 ust. 3 rozporządzenia.

Jednocześnie, na podstawie złożonych przez administratora danych pisemnych wyjaśnień oraz innych nadesłanych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.: administrator danych zaprzestał przetwarzania danych osobowych uczniów nieprzyjętych do szkół dziennych dla młodzieży wchodzących w skład ZSR dłużej niż było to niezbędne do osiągnięcia celu przetwarzania; obecnie dla systemu informatycznego o nazwie „B” stosowane jest ośmioznakowe hasło dostępu; prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych, na którą składa się „Ewidencja osób upoważnionych do przetwarzania danych osobowych” oraz „Ewidencja do przetwarzania danych osobowych w systemach informatycznych”, zawiera informacje o identyfikatorze osoby przetwarzającej dane osobowe w systemie informatycznym.

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. S.A./Sz1029/97).

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