GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 23 października 2014 r.

DIS/DEC-1012/14/82855

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 31 ust. 1 i 2 oraz art. 36 ust. 1-3, art. 37 i art. 39 ust. 1 w zw. z art. 31 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182), a także § 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 IV ust. 2 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Pana D. O. prowadzącego działalność gospodarczą pod firmą C.,

Nakazuję Panu D. O. prowadzącemu działalność gospodarczą pod firmą C. – jako podmiotowi, o którym mowa w art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182), zwanej dalej „ustawą" – usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. **Zaprzestanie przetwarzania danych osobowych, które są pozyskiwane w toku rejestracji użytkownika serwisu internetowego o nazwie [...], bez podstawy prawnej wynikającej z umowy powierzenia przetwarzania danych osobowych, o której mowa**

w art. 31 ust. 1 i 2 ustawy, zawartej na piśmie z administratorem tych danych, tj. E. Sp. z o.o., w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. **Zaprzestanie powierzania spółce h. spółka jawna realizacji zadań związanych z przetwarzaniem danych osobowych pozyskiwanych w związku z funkcjonowaniem serwisu internetowego o nazwie [...] – których administratorem jest E. Sp. z o.o. – bez legitymowania się w tym zakresie podstawą prawną wynikającą z umowy, o której mowa w art. 31 ust. 1 i 2 ustawy, zawartej na piśmie z administratorem tych danych, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
3. **Zastosowanie odpowiednich do zagrożeń środków technicznych w celu ochrony danych osobowych w toku uwierzytelniania użytkowników serwisu internetowego o nazwie [...] oraz podczas wprowadzania i modyfikacji danych osobowych przetwarzanych w ramach kont użytkowników tego serwisu poprzez wprowadzenie środków kryptograficznej ochrony wyżej wskazanych danych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zapewnienie, aby hasło logowania do systemu informatycznego o nazwie A, w którym przetwarzane są dane osobowe użytkowników serwisu internetowego o nazwie [...], było zmieniane nie rzadziej niż co 30 dni, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Opracowanie i wdrożenie dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, o której mowa w art. 36 ust. 2 ustawy, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Wyznaczenie administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy, w terminie 30 od dnia, w którym niniejsza decyzja stanie się ostateczna.**
7. **Zapewnienie, aby dostęp do danych osobowych posiadały wyłącznie osoby upoważnione do przetwarzania danych osobowych, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
8. **Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie z art. 39 ust. 1 ustawy, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę u Pana D. O. prowadzącego działalność gospodarczą pod firmą C. (zwanego dalej również „Przedsiebiorcą"), 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 2014 r. poz. 1182) 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 dane osobowe pozyskiwane za pośrednictwem serwisu [...] przetwarzane przez Pana D. O. prowadzącego działalność gospodarczą pod firmą C.mW toku kontroli odebrano od Przedsiębiorcy 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 Pana D. O.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych objętych zakresem kontroli Pan D. O. prowadzący działalność gospodarczą pod firmą C., naruszył przepisy o ochronie danych osobowych przetwarzając ww. dane jako podmiot, o którym mowa w art. 31 ust. 1 ustawy. Uchybienia te polegały na:

1. Przetwarzaniu danych osobowych, pozyskiwanych w toku rejestracji użytkownika serwisu internetowego o nazwie [...], bez podstawy prawnej wynikającej z umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy, zawartej na piśmie z administratorem tych danych, tj. E. Sp. z o.o.
2. Powierzaniu spółce h. spółka jawna danych osobowych, które są pozyskiwane w toku rejestracji użytkownika serwisu internetowego o nazwie [...], bez podstawy prawnej wynikającej z umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy, zawartej na piśmie z administratorem tych danych, tj. E. Sp. z o.o.
3. Niezastosowaniu odpowiednich do zagrożeń środków technicznych w celu ochrony danych osobowych w toku uwierzytelniania użytkowników serwisu internetowego o nazwie [...] oraz podczas wprowadzania i modyfikacji danych osobowych przetwarzanych w ramach kont użytkowników tego serwisu z uwagi na brak środków kryptograficznej ochrony ww. danych (art. 36 ust. 1 ustawy).

4. Niezapewnieniu, aby hasło logowania do systemu informatycznego o nazwie A, w którym przetwarzane są dane osobowe użytkowników serwisu internetowego o nazwie [...], było zmieniane nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
5. Nieopracowaniu dokumentacji, o której mowa w art. 36 ust. 2 ustawy, opisującej sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.
6. Niewyznaczeniu administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy).
9. Niezapewnieniu, aby dostęp do danych osobowych posiadały wyłącznie osoby upoważnione do przetwarzania danych osobowych (art. 37 ustawy).
7. Nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).

W związku z powyższym, w dniu [...] sierpnia 2014 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma [...]). Pan D. O. prowadzący działalność gospodarczą pod firmą C. – jako podmiot, o którym mowa w art. 31 ust. 1 ustawy – 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 ww. pismo Przedsiębiorca pismem z dnia [...] sierpnia 2014 r. poinformował, iż jest w trakcie usuwania wszystkich stwierdzonych uchybień. Jednocześnie wskazał w nim, iż zarówno techniczne jak i formalne uchybienia zostaną ostatecznie usunięte do dnia [...] września 2014 r. i dopiero z upływem tej daty będzie w stanie przedstawić dowody na potwierdzenie, iż czynności podjęte przez niego w tym zakresie zostały zrealizowane.

Odnosząc się do powyższych wyjaśnień Przedsiębiorcy należy zauważyć, iż samo podjęcie działań w celu zapewnienia, aby dane osobowe w przyszłości były przetwarzane zgodnie z przepisami o ochronie danych osobowych, nie jest wystarczające do uznania, iż uchybienia, o których mowa w zawiadomieniu o wszczęciu postępowania administracyjnego z dnia [...] sierpnia 2014 r. (sygn. pisma [...]), zostały usunięte. Przedsiębiorca do dnia wydania niniejszej decyzji nie przedstawił natomiast żadnych dowodów, które mogłyby stanowić podstawę uznania, iż w zakresie przedmiotowych uchybień przywrócono stan zgodny z prawem.

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

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Jak stanowi ust. 2 powołanego

artykułu podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

Ustalono, iż w dniu [...] lipca 2012 r. Pan D. O. prowadzący działalność gospodarczą pod firmą C. (zwany dalej również „Przedsiębiorcą") zawarł z E. Sp. z o.o. (zwaną dalej także „Spółką") umowę nr [...], której przedmiotem jest utrzymanie na serwerze (hosting) serwisu internetowego [...] oraz utrzymanie na serwerze poczty elektronicznej, dla następujących kont pocztowych: [...] oraz [...] z możliwością dodania nowych kont pocztowych na wniosek Spółki. Ponadto w dniu [...] września 2013 r. Przedsiębiorca zawarł kolejną umowę z ww. Spółką, na podstawie której zlecono C. obsługę serwisu internetowego [...] w zakresie weryfikacji zgłoszeń firm do uczestnictwa w serwisie (telefoniczna i mailowa) oraz doradztwa w zakresie marketingu oraz rozbudowy, usprawnienia funkcjonowania i wyszukiwania błędów technicznych w działaniu serwisu.

Realizacja zobowiązań wynikających z powołanych powyżej umów wiąże się z przetwarzaniem przez Przedsiębiorcę danych osobowych pozyskiwanych w związku funkcjonowaniem serwisu [...]. Jak bowiem ustalono w celu zarejestrowania się w serwisie należy założyć konto firmowe, w którym należy podać następujące dane: nazwa firmy, adres, NIP, hasło, dane osoby do kontaktu, e-mail, telefon kontaktowy oraz opcjonalnie numer licencji posiadanej przez użytkownika. Jednocześnie stwierdzono, iż użytkownikami serwisu mogą być także osoby fizyczne prowadzące indywidualną działalność gospodarczą. W związku z faktem, iż z dniem 1 stycznia 2012 r. uchylono art. 7a ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej (Dz.U. 1999 nr 101 poz. 1178 z późn. zm.), który wyłączał dane osobowe zawarte w ewidencji działalności gospodarczej spod przepisów ustawy o ochronie danych osobowych, ochronie przewidzianej w tej ustawie podlegają obecnie dane osób fizycznych bez względu na to czy osoby te prowadzą działalność gospodarczą, czy też nie. Wskazane powyżej umowy nie zawierają jednak stosownych klauzul w zakresie powierzenia przez Spółkę Przedsiębiorcy przetwarzania ww. danych osobowych, w szczególności nie określają zakresu danych oraz celu ich przetwarzania. Nie mogą być tym samym uznane za umowę, o której mowa w art. 31 ust. 1 ustawy. Zatem na chwilę obecną Pan D. O. prowadzący działalność gospodarczą pod nazwą C. przetwarza wyżej wskazane dane bez podstawy prawnej wynikającej z art. 31 ust. 1 i 2 ustawy.

Ponadto ustalono, iż zgodnie z umową nr [...] zawartą w dniu [...] lipca 2012 r. Spółka zleciła Przedsiębiorcy utrzymanie na serwerze (hosting) serwisu internetowego [...] oraz utrzymanie na serwerze poczty elektronicznej, dla następujących kont pocztowych: [...] oraz[...]. Jak stwierdzono w toku kontroli serwery, na których znajduje się serwis sprawdzkierowce.pl nie są

własnością C. lecz są użytkowane przez Pana D. O. w ramach umowy hostingu o parametrach [...] zawartej przez niego drogą elektroniczną ze spółką h. spółka jawna.

Z uwagi na fakt, iż Pan D. O. jako przedsiębiorca realizujący zobowiązania wynikające z umowy nr [...] zawartej ze Spółką w dniu [...] lipca 2012 r przetwarza dane osobowe pozyskiwane w związku funkcjonowaniem serwisu [...], należy uznać, iż w opisywanym przypadku dochodzi do faktycznego powierzenia Przedsiębiorcy przez Spółkę przetwarzania ww. danych osobowych.

Jak wynika z art. 31 ust. 1 ustawy, uprawnienie do powierzenia przetwarzania danych przysługuje wyłącznie administratorowi danych. Co do zasady nie może tego zatem dokonać podmiot, któremu dane zostały powierzone do przetwarzania. Wyjątek stanowi sytuacja, gdy to sam administrator danych przewidział możliwość dalszego powierzania danych w pisemnej umowie zawartej zgodnie z art. 31 ust. 1 i 2 ustawy. Mówimy wtedy o instytucji tzw. „podpowierzenia" przetwarzania danych osobowych. Należy przy tym zauważyć, iż ww. podpowierzenie może nastąpić jedynie na podstawie zawartej na piśmie umowy, która określi zakres oraz cel przetwarzania danych, tj. przy spełnieniu wymogów wynikających z art. 31 ust. 1 i 2 ustawy.

Mając powyższe na uwadze należy stwierdzić, iż zawarta pomiędzy Spółką a Przedsiębiorcą w dniu [...] lipca 2012 r. umowa nr [...] w zakresie usług hostingu, na podstawie której Przedsiębiorca przetwarza dane osobowe pozyskiwane w związku funkcjonowaniem serwisu [...], nie zawiera w swej treści zakresu i celu przetwarzania danych osobowych, co stanowi *essentialia negotii* umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy. Nie można zatem uznać jej za umowę, na podstawie której administrator danych, działając w oparciu o art. 31 ust. 1 ustawy, powierza innemu podmiotowi przetwarzanie danych osobowych. Z powołanej umowy nie wynika również, iż hosting serwisu internetowego [...], stanowiący przedmiot tej umowy, może być świadczony przez Przedsiębiorcę z wykorzystaniem serwerów podmiotu zewnętrznego. Mimo to Przedsiębiorca, realizując ww. umowę korzysta z serwerów h. spółka jawna, przez co faktycznie podpowierza wyżej wskazanej spółce dane osobowe pozyskiwane w ramach serwisu. Zatem należy uznać, iż powyższe podpowierzenie danych osobowych odbywa się z naruszeniem art. 31 ust. 1 i 2 ustawy.

Z uwagi jednak na to, iż Przedsiębiorcy – pomimo wyżej wskazanych uchybień dotyczących podstawy prawnej powierzenia – faktycznie powierzono przetwarzanie danych osobowych, których administratorem jest E. Sp. z o.o., należy wskazać, iż zgodnie z art. 31 ust. 3 ustawy, podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

Zgromadzony w sprawie materiał dowodowy wskazuje, iż Przedsiębiorca naruszył przepisy o zabezpieczeniu danych osobowych zawarte w art. 36 ust. 1-3, art. 37 oraz art. 39 ust. 1 ustawy.

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.

W części A pkt IV ust. 2 załącznika do rozporządzenia wskazano zaś, iż w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni.

Z ustaleń dokonanych podczas kontroli wynika, iż nie zastosowano środków kryptograficznej ochrony danych w toku uwierzytelniania użytkowników serwisu [...] oraz podczas wprowadzania i modyfikacji danych osobowych przetwarzanych w ramach kont użytkowników serwisu.

Ponadto hasło logowania do systemu informatycznego o nazwie A, w którym przetwarzane są dane osobowe użytkowników serwisu, wykorzystywane przez Panią J. C. nie jest zmieniane.

Zatem w opisanych powyżej przypadkach nie zastosowano środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

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". Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Dokumentacja, o której jest mowa wyżej, zgodnie z ust. 3, wdraża administrator danych.

Przeprowadzona kontrola wykazała, iż Przedsiębiorca nie opracował polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, o których mowa w § 3 ust. 1 rozporządzenia.

Zgodnie z art. 36 ust. 3 ustawy, administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

Jak stwierdzono Przedsiębiorca nie powołał administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Ustalono, iż osobie, która w C. została dopuszczona do przetwarzania danych osobowych nie zostało nadane upoważnienie do przetwarzania tych danych.

Zgodnie z art. 39 ust. 1 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Stwierdzono, iż Przedsiębiorca nie prowadzi ewidencji osób upoważnionych do przetwarzania danych osobowych.

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.

W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r., Nr 229, poz. 1954 z późn. zm.).