GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 28 października 2014 r.

DIS/DEC-1022/14/84106

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, art. 24 ust. 1, art. 25 ust. 1, art. 36 ust. 1, 36 ust. 2, art. 36 ust. 3 i art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182), zwanej dalej ustawą o ochronie danych osobowych, 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 E. Sp. z o.o.,

Nakazuję E. Sp. z o.o. (zwanej dalej również „Spółką") usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. **Zaprzestanie powierzania przetwarzania danych osobowych pozyskiwanych w toku rejestracji użytkownika serwisu internetowego o nazwie [...] Panu D. O. prowadzącemu działalność gospodarczą pod firmą C. oraz h. spółka jawna, bez zawarcia z wyżej wskazanymi podmiotami pisemnych umów powierzenia przetwarzania ww. danych osobowych zgodnie z art. 31 ust. 1 ustawy o ochronie danych osobowych, określających cel i zakres, w jakim podmioty te mogą przetwarzać powierzone dane osobowe, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**

2. **Realizowanie wobec użytkowników serwisu internetowego o nazwie [...], obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
3. **Realizowanie wobec osób wskazanych przez użytkowników serwisu internetowego o nazwie [...], jako właściwe do kontaktu, obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **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.**
5. **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.**
6. **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 o ochronie danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
7. **Wyznaczenie administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy o ochronie danych osobowych, w terminie 30 od dnia, w którym niniejsza decyzja stanie się ostateczna.**
8. **Zgłoszenie Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji zbioru danych osobowych pozyskiwanych w związku z rejestracją użytkowników serwisu internetowego o nazwie [...], w terminie 30 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 w E. Sp. z o.o. (zwanej dalej również „Spółką"), w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt [...]), tj. ustawą o ochronie danych osobowych 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 przetwarzane przez E. Sp. z o.o., w związku z prowadzeniem serwisu internetowego dostępnego pod adresem [...] – kontrola z urzędu w związku z pismami Departamentu Orzecznictwa Legislacji i Skarg z dnia [...] lutego 2013 r. (znak: ...]) i z dnia [...] września 2013 r. (znak: [...]) oraz w związku z pismem Zespołu Rzecznika Prasowego z dnia [..] grudnia 2013 r. (znak: [...]), a także w związku z kontrolą [...]. W toku kontroli odebrano od Prezesa Zarządu 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. Powierzaniu przetwarzania danych osobowych pozyskiwanych w toku rejestracji użytkownika serwisu internetowego o nazwie [...] Panu D. O. prowadzącemu działalność gospodarczą pod firmą C. oraz h. spółka jawna, bez zawarcia z ww. podmiotami pisemnych umów w zakresie powierzenia przetwarzania wyżej wskazanych danych osobowych (art. 31 ust. 1 i 2 ustawy o ochronie danych osobowych).
2. Nierealizowaniu wobec użytkowników serwisu internetowego o nazwie [...], obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych.
3. Nierealizowaniu wobec osób wskazanych przez użytkowników serwisu internetowego o nazwie [...] jako właściwe do kontaktu, obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych.
4. 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 o ochronie danych osobowych).

5. 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).
6. Nieopracowaniu dokumentacji, o której mowa w art. 36 ust. 2 ustawy o ochronie danych osobowych, opisującej sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.
7. Niewyznaczeniu administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy o ochronie danych osobowych).
8. Niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji zbioru danych osobowych pozyskiwanych w związku z rejestracją użytkowników serwisu internetowego o nazwie [...] (art. 40 ustawy o ochronie danych osobowych).

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 [...]). Spółka, jako administrator danych, została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Z powyższego prawa Spółka nie skorzystała.

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

1. Zgodnie z art. 31 ust. 1 ustawy o ochronie danych osobowych, 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.

   Przeprowadzona kontrola wykazała, iż na podstawie umowy nr [...] z dnia [...] lipca 2012 r. E. Sp. z o.o., zleciła Panu D. O. prowadzącemu działalność gospodarczą pod firmą C., zwanemu dalej również „Zleceniobiorcą", 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. W toku kontroli przeprowadzonej u Zleceniobiorcy (sygn. akt [...]) ustalono natomiast, iż serwery, na których znajduje się serwis [...] (zwany dalej również „serwisem") nie są własnością C. lecz są użytkowane przez ww. Zleceniobiorcę w ramach umowy hostingu o parametrach [...] zawartej przez niego drogą elektroniczną z h. spółka jawna. Ponadto ustalono, iż w dniu [...] września 2013 r. Spółka zawarła kolejną umowę ze Zleceniobiorcą, na podstawie której zleciła mu obsługę serwisu internetowego

[...] w zakresie weryfikacji zgłoszeń podmiotów gospodarczych do uczestnictwa w serwisie (telefoniczna i mailowa) oraz doradztwa w zakresie marketingu oraz rozbudowy, usprawnienia funkcjonowania i wyszukiwania błędów technicznych w działaniu serwisu.

Jak 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 również dane osób fizycznych prowadzących działalność gospodarczą. Administrator danych osób fizycznych prowadzących działalność gospodarczą zobowiązany jest więc do spełnienia wobec tych osób obowiązków wynikających z przepisów ustawy o ochronie danych osobowych.

Zgodnie z art. 31 ust. 1 ustawy o ochronie danych osobowych, 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 o ochronie danych osobowych i może nastąpić jedynie na podstawie zawartej na piśmie umowy między podmiotem, któremu powierzono przetwarzanie danych osobowych a kolejnym podmiotem, która określi zakres oraz cel przetwarzania danych, tj. przy spełnieniu wymogów wynikających z powołanych przepisów.

W toku kontroli Pan E. K., Prezes Zarządu Spółki, wyjaśnił, iż Spółka nie zawarła ze Zleceniobiorcą odrębnej umowy powierzenia przetwarzania danych osobowych (w odniesieniu do danych osób fizycznych pozyskiwanych przez Spółkę w toku rejestracji użytkownika serwisu [...]). Należy jednocześnie wskazać, iż żadna z powołanych powyżej umów, na podstawie których Zleceniobiorca uzyskał dostęp do ww. danych osobowych nie zawiera w swej treści zakresu i celu przetwarzania danych osobowych (essentialia negotii umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych). Podkreślenia wymaga również fakt, iż z umowy nr [...] nie wynika, aby usługa hostingu serwisu internetowego [...], stanowiąca przedmiot tej umowy,

mogła być świadczona przez Zleceniobiorcę z wykorzystaniem serwerów podmiotu zewnętrznego.

Należy zatem stwierdzić, iż powierzenie przetwarzania danych osobowych, pozyskiwanych przez Spółkę w toku rejestracji użytkownika serwisu [...], Panu D. O. prowadzącemu działalność gospodarczą pod firmą C. oraz h. spółka jawna odbywa się z naruszeniem art. 31 ust.1 i 2 ustawy o ochronie danych osobowych.

2. Zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W toku kontroli ustalono, iż Spółka nie realizuje wobec użytkowników serwisu [...] obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych.

3. Zgodnie z art. 25 ust. 1 ustawy o ochronie danych osobowych, w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, 3) źródle danych, 4) prawie dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

W toku kontroli ustalono, iż Spółka nie realizuje wobec osób wskazanych przez użytkowników serwisu [...] jako właściwe do kontaktu, obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych.

4. Zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych, 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.

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

5. 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.

   W toku kontroli ustalono, iż hasło logowania do systemu informatycznego o nazwie A, w którym przetwarzane są dane osobowe użytkowników serwisu [...], jest zmieniane raz na pół roku.

6. Zgodnie z art. 36 ust. 2 ustawy o ochronie danych osobowych, 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. 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, powinna zostać wdrożona przez administratora danych.

   W toku kontroli stwierdzono, że Spółka nie prowadzi dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, naruszając tym samym art. 36 ust. 2 ustawy o ochronie danych osobowych.

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

   Stwierdzono, iż w Spółce nie wyznaczono osoby pełniącej obowiązki administratora bezpieczeństwa informacji.

8. Zgodnie z art. 40 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. Jak stanowi natomiast art. Art. 7 pkt 1 powołanej ustawy, ilekroć w ustawie jest mowa o zbiorze danych rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

W toku kontroli stwierdzono, iż Spółka w związku z prowadzeniem serwisu internetowego dostępnego pod adresem [...] przetwarza dane osobowe, które pozyskuje w toku rejestracji kont użytkowników tego serwisu. Ustalono, iż rejestracja konta użytkownika serwisu składa się z dwóch etapów. Pierwszy polega na wypełnieniu na stronie serwisu elektronicznego formularza o nazwie „Załóż konto firmowe". W opisywanym formularzu potencjalny użytkownik podaje następujące dane: nazwa firmy, adres, NIP, nr licencji, hasło, dane osoby do kontaktu, e-mail, telefon kontaktowy. Jedynie numer licencji jest informacją, której wprowadzenie jest opcjonalne. Natomiast drugi etap to tzw. weryfikacja potencjalnego użytkownika, którą w imieniu Spółki zajmuje się Pan D. O. prowadzący działalność gospodarczą pod firmą C. Opisywana weryfikacja odbywa się na podstawie informacji podanych w formularzu rejestracyjnym, dokumentów przesłanych przez potencjalnego użytkownika potwierdzających prowadzenie przez niego działalności gospodarczej oraz na podstawie rozmowy telefonicznej z takim użytkownikiem. Do czasu zakończenia ww. weryfikacji konto użytkownika serwisu jest nieaktywne (nie można się na nie zalogować).

Jak ustalono przetwarzanie przez Spółkę danych osobowych pozyskiwanych w toku rejestracji kont użytkowników serwisu obywa się w celu zapewnienia możliwości kontaktu, przeprowadzenia weryfikacji użytkownika, aktywacji jego konta oraz umożliwienia mu korzystania z pełnych funkcjonalności serwisu [...].

Nie ulega zatem wątpliwości, iż Spółka w związku z funkcjonowaniem serwisu [...] przetwarza w zbiorze danych dane osób fizycznych prowadzących działalność gospodarczą (w zakresie: firma, adres, NIP, nr licencji) oraz tzw. dane kontaktowe (w zakresie: imię, nazwisko, e-mail, nr telefonu) osób fizycznych wskazanych przez użytkownika (może to być sam przedsiębiorca lub inna osoba). Spółka nie zgłosiła jednak ww. zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Z uwagi na fakt, iż w opisywanym przypadku nie zachodzą przesłanki wskazane w art. 43 ust. 1 pkt 1 - 11 ustawy o ochronie danych osobowych, Spółka nie zgłaszając ww. zbioru naruszyła obowiązek, o którym mowa w art. 40 tej ustawy.

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.).