GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Warszawa, dnia 3 kwietnia 2015 r.

DIS/DEC-302/15/27465

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 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i 6 oraz art. 22 w związku z art. 26 ust. 1 pkt 1, art. 31 ust. 1 i 2 oraz art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz § 7 ust. 1 pkt 1 i 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 T. Sp. z o.o.,

Nakazuję T. Sp. z o.o. usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. **Zaprzestanie udostępniania TM. danych osobowych bez podstawy prawnej, tj. bez zawarcia z ww. podmiotem umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.), określającej cel i zakres, w jakim TM. może przetwarzać powierzone jej dane osobowe, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Zaprzestanie pozyskiwania od osób zatrudnionych w T. Sp. z o.o. informacji o wzroście w cm i kolorze oczu, od dnia, w którym niniejsza decyzja stanie się ostateczna.**

ul. Stawki 2
00-193 Warszawa

tel. 860-70-81
fax 860-70-90
www.giodo.gov.pl

3. **Usunięcie zgromadzonych informacji o wzroście w cm i kolorze oczu osób zatrudnionych w T. Sp. z o.o., w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zastosowanie środków technicznych w celu ochrony danych osobowych pracowników T. Sp. z o.o. przesyłanych w sieci publicznej do TMM Sp. z o.o., w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Zmodyfikowanie plików […], w których przetwarzane są dane osobowe pracowników T. Sp. z o.o., w taki sposób, aby zapewniały dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz sporządzenie i wydrukowanie raportu zawierającego ww. informacje w powszechnie zrozumiałej formie, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Zmodyfikowanie systemu informatycznego o nazwie „A" (służącego do przetwarzania danych osobowych pracowników T. Sp. z o.o. w związku z funkcjonującym systemem kontroli dostępu), w taki sposób, aby zapewniał dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu oraz sporządzenie i wydrukowanie raportu zawierającego ww. informacje w powszechnie zrozumiałej formie, w terminie 3 miesięcy 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 w T. Sp. z o.o., zwanej dalej Spółką, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych ([…]), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 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 rozporządzeniem. Zakresem kontroli objęto przetwarzanie danych osobowych osób zatrudnionych w Spółce. 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 Dyrektora Oddziału 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. Udostępnianiu danych osobowych bez podstawy prawnej TM., w związku z brakiem umowy powierzenia przetwarzania danych osobowych zawartej z ww. podmiotem (art. 26 ust. 1 pkt 1 ustawy i art. 31 ust. 1 i 2 ustawy).
2. Gromadzeniu przez Spółkę danych osobowych osób zatrudnionych w zakresie wykraczającym (o wzrost w cm i kolor oczu) poza zakres dopuszczony na podstawie przepisów Kodeksu pracy (art. 26 ust. 1 pkt 1 ustawy).
3. Wysyłaniu za pomocą poczty elektronicznej do TMM Sp. z o.o. dokumentów zawierających dane osobowe pracowników Spółki bez zabezpieczenia przed ich udostępnieniem osobom nieupoważnionym (art. 36 ust. 1 ustawy).
4. Niezapewnianiu przez pliki […], w których przetwarzane są dane osobowe pracowników Spółki, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz sporządzenia i wydrukowania raportu zawierającego ww. informacje w powszechnie zrozumiałej formie (§ 7 ust. 1 pkt 1 i 2 oraz § 7 ust. 3 rozporządzenia).
5. Niezapewnianiu przez system informatyczny o nazwie „A” (służący do przetwarzania danych osobowych pracowników Spółki w związku z funkcjonującym systemem kontroli dostępu) odnotowania daty pierwszego wprowadzenia danych do systemu oraz sporządzenia i wydrukowania raportu zawierającego ww. informacje w powszechnie zrozumiałej formie (§ 7 ust. 1 pkt 1 oraz § 7 ust. 3 rozporządzenia).

W związku z powyższym, w dniu […] marca 2015 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma […]).

Spółka nie ustosunkowała się pisemnie do stwierdzonych uchybień w procesie przetwarzania danych osobowych, stanowiących przedmiot postępowania administracyjnego, wymienionych w zawiadomieniu o wszczęciu postępowania.

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

Stosownie do art. art. 26 ust. 1 pkt 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem.

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

W toku kontroli ustalono, iż Spółka powierza przetwarzanie danych osobowych pracowników TM dla celów związanych z naliczaniem i wypłatą wynagrodzenia, w tym premii, oraz dokonywaniem oceny pracownika. Ponadto ustalono, że TM jest odpowiedzialna za zarządzanie komputerami, które są wykorzystywane do przetwarzania danych osobowych pracowników Spółki, w związku z czym ma dostęp do danych ww. osób. Z TM. Spółka nie zawarła jednak żadnej umowy, która regulowałaby w jakim zakresie oraz w jakim celu ten podmiot może przetwarzać dane osobowe osób zatrudnionych w Spółce.

Wobec powyższego, powierzenie przetwarzania danych osobowych TM. przez Spółkę bez zawarcia umowy, o której mowa w art. 31 ust. 1 ustawy, stanowi działanie niezgodne z prawem.

Zgodnie z art. 26 ust. 1 pkt 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem. Stosownie do art. 22^1 § 1, § 2, § 4, § 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2014 r., Nr 1502), pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko; 2) imiona rodziców; 3) datę urodzenia; 4) miejsce zamieszkania (adres do korespondencji); 5) wykształcenie; 6) przebieg dotychczasowego zatrudnienia. Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także: 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy; 2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL). Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 2. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. W zakresie nieuregulowanym w § 1-4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

W toku kontroli ustalono, że Spółka wykonuje kserokopie dowodów osobistych pracowników, na których żadne dane nie są anonimizowane (np. poprzez ich zamazanie). Wykonywanie ww. kserokopii powoduje gromadzenie przez Spółkę danych osobowych osób zatrudnionych w zakresie wykraczającym (o wzrost w cm i kolor oczu) poza zakres dopuszczony na

podstawie powołanych wyżej przepisów Kodeksu pracy. Jednocześnie nie wskazano żadnych odrębnych przepisów, które pozwalałyby Spółce zbierać te dane. Tym samym dochodzi do naruszenia powołanych wyżej przepisów ustawy o ochronie danych osobowych i Kodeksu pracy.

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 toku kontroli ustalono, że Spółka za pomocą poczty elektronicznej wysyła do TMM Sp. z o.o. dokumenty zawierające dane osobowe jej pracowników. Wysyłane są dokumenty w formie plików […] jako załączniki do przesyłanej wiadomości. Pliki takie nie są zabezpieczane hasłem, a transmisja przesyłanych danych nie jest szyfrowana (zabezpieczona kryptograficznie).

W związku z powyższym należy uznać, że Spółka w ww. zakresie nie zastosowała środków technicznych zapewniających ochronę przetwarzanych danych osobowych, o których mowa w art. 36 ust. 1 ustawy.

Stosownie z § 7 ust. 1 pkt 1 i 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 i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

Kontrola wykazała, że pliki […], w których przetwarzane są dane osobowe pracowników Spółki, nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

W toku kontroli ustalono ponadto, że system informatyczny o nazwie „A” (służący do przetwarzania danych osobowych pracowników Spółki w związku z funkcjonującym systemem kontroli dostępu) nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu.

W związku z powyższym należy uznać, że w omawianym zakresie ww. systemy informatyczne nie spełniają wymogów wynikających z powołanego przepisu rozporządzenia.

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 przeprowadzonej kontroli ustalono, że pliki […], w których przetwarzane są dane osobowe pracowników Spółki, nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu i identyfikatorze użytkownika wprowadzającego dane osobowe do systemu – załącznik nr […] do protokołu kontroli (protokół oględzin).

Kontrola także wykazała, że system informatyczny o nazwie „A" (służący do przetwarzania danych osobowych pracowników Spółki w związku z funkcjonującym systemem kontroli dostępu) nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informację o dacie pierwszego wprowadzenia danych do systemu.

W związku z powyższym należy uznać, że w omawianym zakresie ww. systemy informatyczne nie spełniają wymogów wynikających z powołanego przepisu rozporządzenia.

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

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych i 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 2012 r., poz. 1015 z późn. zm.).