



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

Warszawa, dnia 25 sierpnia 2015 r.

DESiWM/DEC-690/15

Dotyczy sprawy: [...]

DECYZJA

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267), oraz art. 12 pkt 2 i art. 48 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.), zwanej dalej ustawą, po przeprowadzeniu postępowania administracyjnego na wniosek A. (...) Sp. z o.o., z siedzibą w W. (...), zwaną dalej Wnioskodawcą lub Spółką, w sprawie zatwierdzenia wiążących reguł korporacyjnych, zwanych dalej WRK, dotyczących przekazywania danych osobowych do odbiorców z siedzibami w państwach trzecich, należących do grupy kapitałowej A. (...), zwanej dalej Grupą A. (...),

zatwierdzam wiążące reguły korporacyjne przyjęte w ramach grupy kapitałowej A. (...).

Uzasadnienie

Do Generalnego Inspektora wpłynął wniosek złożony przez Wnioskodawcę, o zatwierdzenie wiążących reguł korporacyjnych przyjętych w ramach grupy kapitałowej A. (...).

Po zapoznaniu się z przedstawionymi przez Wnioskodawcę dokumentami, Generalny Inspektor ustalił, co następuje:

- 1) Wnioskodawca oraz Odbiorcy należą do Grupy A. (...);
- 2) Wnioskodawca przedstawił WRK przyjęte przez Grupę A. (...);

- 3) WRK zostały przygotowane zgodnie z właściwymi dokumentami Grupy Roboczej ds. ochrony danych (Grupy Roboczej Art. 29), ustanowionej na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281, z 23.11.1995), zwanej dalej dyrektywą, tj.: Dokumentem roboczym dotyczącym przekazywania danych osobowych do krajów trzecich: zastosowanie Art. 26 ust. 2 dyrektywy UE w sprawie ochrony danych w odniesieniu do wiążących reguł korporacyjnych zobowiązujących przedsiębiorstwa do ich stosowania przy międzynarodowym przepływie danych (WP 74), Dokumentem roboczym dotyczącym gwarancji wynikających z wiążących reguł korporacyjnych (WP 107), Dokumentem roboczym dotyczącym ustanowienia wzorcowej listy kontrolnej dla wniosków o zatwierdzenie wiążących reguł korporacyjnych” (WP 108), Rekomendacji w sprawie standardowego wniosku o zatwierdzenie wiążących reguł korporacyjnych dla przekazywania danych osobowych (WP 133), Dokumentem roboczym ustanawiającym tabelę zawierającą elementy i zasady, które mają być uwzględnione w wiążących regułach korporacyjnych (WP 153), Dokumentem roboczym w sprawie określenia ram dla struktury wiążących reguł korporacyjnych (WP 154), oraz Dokumentem roboczym w sprawie często zadawanych pytań dotyczących wiążących reguł korporacyjnych (WP 155), co zostało potwierdzone w trakcie procedury współpracy, przeprowadzonej w ramach Grupy Roboczej Art. 29, w celu stwierdzenia, czy WRK spełniają wymogi art. 26 ust. 2 dyrektywy, tj.: czy zapewniają odpowiednie zabezpieczenia odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw;
- 4) Organ ochrony danych osobowych z Wielkiej Brytanii po przeprowadzeniu stosownej procedury zatwierdził w dniu 24 grudnia 2014 r. przedmiotowe WRK zgodnie z przepisami krajowej ustawy o ochronie danych osobowych;
- 5) WRK dotyczą przekazania danych osobowych: pracowników, pracowników branży medycznej (w większości wypadków są to klienci), dostawców i pacjentów.
- 6) Celem przekazywania danych pracowników są:
- a) planowanie zespołów sprzedażowych;
 - b) badania skuteczności zespołów sprzedażowych;
 - c) zarządzania projektami;
 - d) rozwijanie umiejętności;
 - e) rekrutacja;
 - f) zarządzanie wynagrodzeniami i kosztami;
 - g) zarządzanie świadczeniami;

- h) planowanie podróży służbowych;
 - i) zarządzanie urlopami chorobowymi i nieobecnością pracowników;
 - j) zarządzanie wydajnością
 - k) planowanie ścieżek kariery;
 - l) monitoring kwalifikacji;
 - m) planowanie zmian kadrowych;
 - n) programy rozwoju i szkoleń;
 - o) procedury dyscyplinarne, zarządzanie możliwościami i rozpatrywanie skarg;
 - p) zarządzanie kwestiami stosunku pracy;
 - q) działania w zakresie monitorowania i utrzymania;
 - r) zarządzanie pracownikami oddelegowanymi za granicę;
 - s) rozwiązanie stosunku pracy i przejście na emeryturę;
 - t) monitorowanie przyjmowanych pacjentów;
 - u) tworzenie systemów IT;
 - v) zarządzanie IT;
- 7) Celem przekazywania danych przedstawicieli branży medycznej są:
- a) obsługa klienta;
 - b) szkolenia dotyczące produktów i leczenia;
 - c) marketing;
 - d) zarządzanie relacjami z klientem;
 - e) zarządzanie kluczowymi środowiskami opiniotwórczymi;
 - f) relacja odbiorca płatności/płatnik;
 - g) badania kliniczne;
 - h) kluczowe działania w zakresie badania i rozwoju;
 - i) bezpieczeństwo leków;
 - j) zarządzanie zewnętrznymi badaczami;
 - k) ocena jakości;
 - l) bezpieczeństwo lub skuteczność produktów i leczenia;
 - m) badanie due diligence;
 - n) zarządzanie inwestorami;
 - o) realizacja transakcji;
- 8) Celem przekazywania danych dostawców są:
- a) zarządzanie kontaktami biznesowymi;
 - b) zarządzanie aktywami trwałymi;

- c) proces od zakupu do zapłaty;
 - d) tworzenie systemów IT;
 - e) zarządzanie IT;
 - f) badanie due diligence;
 - g) zarządzanie udziałowcami/inwestorami;
 - h) monitorowanie działań;
 - i) monitorowanie przyjmowanych pacjentów;
 - j) badanie due diligence sprzedawców i dostawców;
 - k) zarządzanie sprzedawcami i dostawcami;
 - l) procesy umowne;
- 9) Celem przekazywania danych pacjentów są:
- a) badania kliniczne;
 - b) kluczowe działania w zakresie badania i rozwoju;
 - c) bezpieczeństwo leków;
 - d) tworzenie systemów IT;
 - e) zarządzanie IT
 - f) monitorowanie działań.

Po zapoznaniu się z całością zgromadzonego w sprawie materiału dowodowego Generalny Inspektor zważył, co następuje:

Stwierdzić należy, że w myśl art. 6 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267), zwanym dalej kpa, organy administracji publicznej działają na podstawie przepisów prawa. Stosownie zaś do art. 104 § 1 kpa organ administracji publicznej załatwia sprawę przez wydanie decyzji, chyba że przepisy kodeksu stanowią inaczej.

Zgodnie z art. 48 ust. 3 ustawy Generalny Inspektor zatwierdza w drodze decyzji administracyjnej, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do celów przekazania danych osobowych przez administratora danych lub podmiot, o którym mowa w art. 31 ust. 1 ustawy, do należącego do tej samej grupy innego administratora danych lub podmiotu, o którym mowa w art. 31 ust. 1 ustawy, w państwie trzecim. Dodatkowo zgodnie z art. 48 ust. 4 ustawy Generalny Inspektor przed zatwierdzeniem WRK może przeprowadzić konsultacje z właściwymi organami ochrony danych osobowych państw należących do Europejskiego Obszaru Gospodarczego, na którym terytorium mają siedziby przedsiębiorcy należący do grupy, o której mowa w ust. 3, przekazując im niezbędne informacje w tym celu. Dodatkowo zgodnie z art. 48 ust

5 ustawy Generalny Inspektor, wydając decyzję dotyczącą zatwierdzenia WRK, uwzględni wyniki przeprowadzonych konsultacji, o których mowa w ust. 4, a jeżeli WRK były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego – może uwzględnić to rozstrzygnięcie.

Generalny Inspektor, rozpatrując wnioski o zatwierdzenie WRK, jest zobowiązany ustalić, czy ich treść jest zgodna z dokumentami Grupy Roboczej Art. 29, tj. WP 74, WP 107, WP 108, WP 133, WP 153, WP 154 oraz WP 155. Podkreślenia wymaga, że WRK są: „wiązące” lub „możliwe do wyegzekwowania na drodze prawnej”, ponieważ tylko instrument mający ten charakter może być uznany za „wystarczające gwarancje” w rozumieniu art. 26 ust. 2 dyrektywy 95/46/WE; ‘korporacyjne’, ponieważ chodzi o reguły obowiązujące wewnątrz korporacji (koncernu) międzynarodowej, na ogół opracowane w siedzibie głównej; oraz stosowane przy międzynarodowych transferach danych, ponieważ w tym tkwi sens istnienia tych reguł.

Biorąc pod uwagę, że WRK w zamierzeniu mają mieć charakter globalny, organy ochrony danych osobowych z państw członkowskich Unii Europejskiej przyjęły skoordynowaną procedurę oceny, mającą na celu umożliwienie wypracowania przez zainteresowaną korporację jednolitego instrumentu prawnego, który będzie miał zastosowanie do międzynarodowych transferów danych w ramach korporacji oraz będzie spełniał wymogi dotyczące ochrony danych osobowych wynikające z przepisów dyrektywy, w tym z jej art. 26 ust. 2.

Pomyślne przejście takiej procedury jest warunkiem *sine qua non* uznania WRK przez krajowy organ ochrony danych osobowych z państwa członkowskiego UE za zapewniające odpowiednie gwarancje w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

Wobec faktu przedłożenia przez Spółkę WRK, które zostały przygotowane zgodnie z ww. dokumentami Grupy Roboczej Art. 29, a także zostały zatwierdzone przez organ ochrony danych osobowych Wielkiej Brytanii, Generalny Inspektor stwierdził w przedmiotowej sprawie spełnienie wymogów art. 48 ust. 3 ustawy. Dodatkowo należy wskazać, że Generalny Inspektor brał udział w skoordynowanej procedurze oceny przedłożonych przez Spółkę WRK, a także może on uwzględnić rozstrzygnięcie organu ochrony danych osobowych Wielkiej Brytanii w tym zakresie.

W tym miejscu należy wyjaśnić, że zatwierdzenie instrumentu, jakim są WRK, oznacza, że zostały zapewnione odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. Tym samym zgodnie z art. 48 ust. 2 pkt 2 ustawy nie jest wymagana zgoda Generalnego Inspektora na poszczególne transfery danych do państw trzecich, które będą się odbywać w ramach zatwierdzonych WRK, a także ze względu na to, że ten sam instrument może być zastosowany przez innych administratorów z Grupy A. (...), posiadających

siedzibę na terytorium Rzeczypospolitej Polskiej, nie muszą oni występować do Generalnego Inspektora z odrębnymi wnioskami o zatwierdzenie WRK.

Jednocześnie należy wskazać, że wszelkie transfery danych osobowych na podstawie WRK mogą nastąpić dopiero po wdrożeniu WRK przez poszczególnych administratorów z Grupy A. (...). Natomiast w ramach określonych przez WRK możliwe są przyszłe operacje przekazywania danych, których konkretyzacja może dopiero nastąpić w przyszłości ze względu na określone okoliczności faktyczne. Niemniej administratorzy z Grupy A. (...), posiadający siedzibę na terytorium Rzeczypospolitej Polskiej, którzy zamierzają przekazywać dane osobowe na podstawie WRK nie mają tutaj dowolności i ich działania są związane z koniecznością spełnienia pozostałych wymogów ustawy. Ustawa, wprowadzając bowiem w swym rozdziale 7 (art. 47 i 48) szczególny reżim dotyczący przekazywania danych osobowych do państw trzecich, nie wyłączyła zastosowania w takich wypadkach pozostałych przepisów ustawy. Przepisy art. 47 i 48 ustawy wprowadzają bowiem jedynie dodatkowe wymogi, które należy spełnić, gdy zamierza się przekazywać dane osobowe do państwa trzeciego. Konieczność ich wypełnienia nie zwalnia administratora danych z pozostałych obowiązków nałożonych na niego przepisami ustawy m.in. w zakresie ich legalności, adekwatności, czy obowiązku zgłoszenia prowadzonych zbiorów danych osobowych do rejestracji. Jednocześnie istotne jest to, że przedmiotem przekazania mogą być dane osobowe tylko w takim zakresie, w jakim ich przetwarzanie przez daną spółkę z Grupy A. (...) na terytorium RP jest dopuszczalne w świetle polskiego prawa.

W tym miejscu podkreślić należy, że decyzja Generalnego Inspektora w przedmiocie zatwierdzenia WRK nie legalizuje wcześniejszego przekazywania danych osobowych do państwa trzeciego, które ewentualnie miałyby miejsce przed datą wydania decyzji w przedmiotowej sprawie. W konsekwencji, rozpoczęcie operacji przekazywania danych osobowych do państwa trzeciego może nastąpić dopiero po wydaniu stosownej decyzji przez Generalnego Inspektora.

Z uwagi na powyższe, wobec zaistnienia odpowiednich przesłanek rozstrzygnięcia niniejszego postępowania administracyjnego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych stronie niezadowolonej z niniejszej decyzji przysługuje, w terminie 14 dni od dnia jej doręczenia, prawo złożenia do Generalnego Inspektora Ochrony Danych Osobowych wniosku o ponowne rozpatrzenie sprawy (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa).