Xawery Konarski

Nowe zasady organizacji ochrony danych osobowych

Z dniem 1 stycznia 2015 r. weszły w życie nowe przepisy dotyczące ochrony danych osobowych, które – jako *lex generali* – mają bezpośrednie zastosowanie do przetwarzania danych osobowych przez zakłady ubezpieczeń i reasekuracji oraz pośredników ubezpieczeniowych. Przepisy te mają odciążyć przedsiębiorców przetwarzających dane osobowe od szeregu powinności o biurokratycznym charakterze. Jednocześnie jednak – w miejsce dotychczasowych – wprowadzono nowe obowiązki dla administratorów danych osobowych. Nowelizacja określiła nowy status i nowe zadania administratora bezpieczeństwa informacji, który ma podlegać bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Wprowadzono także dwa nowe zwolnienia z obowiązku rejestracji zbiorów danych osobowych w Generalnym Inspektoracie Ochrony Danych Osobowych (GIODO).

Słowa kluczowe: rejestr GIODO, administrator bezpieczeństwa informacji, administrator danych osobowych, kontrola funkcjonalna, transfer danych osobowych do państw trzecich.

1. Wprowadzenie

Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[1] w art. 9 dokonała istotnej nowelizacji ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[2]. Przepisy nowelizacji (określanej w niniejszym artykule również jako „nowela u.o.d.o.", „nowe przepisy u.o.d.o.") weszły w życie w dniu 1 stycznia 2015 r. Można je podzielić na trzy podstawowe grupy. Pierwsza z nich dotyczy zasad organizacji ochrony danych osobowych (art. 36a i n.). Drugą grupę stanowią regulacje wprowadzające nowe zasady dotyczące obowiązku zgłoszeń zbiorów danych do rejestru prowadzonego przez Generalnego Inspektora Danych Osobowych (art. 43 ust. 1 pkt 12 oraz art. 43 ust.1a). Ostatnia zmiana dotyczy zasad przekazywania (transferu) danych osobowych z terytorium Polski do państw trzecich (art. 48)[3].

Nowe przepisy ustawy o ochronie danych osobowych w sposób istotny wpływają na działalność podmiotów ubezpieczeniowych, w szczególności zakładów ubezpieczeń i reasekuracji oraz pośredników ubezpieczeniowych. Zawarte w nich regulacje nie dotyczą bowiem materii będącej przedmiotem szczególnych postanowień ustawy o działalności ubezpieczeniowej[4], zgodnie z treścią art. 5 u.o.d.o. znajdują więc – jako *lex generali* – bezpośrednie zastosowanie do przetwarzania danych osobowych przez te podmioty.

[1] Dz. U. z 2014 r. poz.1662.
[2] Tekst jedn. Dz. U. z 2014 r. poz. 1182, z późn. zm.
[3] Definicja legalna „państwa trzeciego" zawarta jest w art. 7 pkt 7 u.o.d.o. (*„państwo nienależące do Europejskiego Obszaru Gospodarczego"*).
[4] Tekst jedn. Dz. U. z 2013 r. poz. 950, z późn. zm.

2. Geneza, cel i ocena nowelizacji

Nowe przepisy ustawy o ochronie danych osobowych zostały przyjęte w ramach tzw. ustawy deregulacyjnej. Ich podstawowym celem było bowiem wprowadzenie rozwiązań odciążających przedsiębiorców przetwarzających dane osobowe od wielu obowiązków o charakterze biurokratycznym. Z tych właśnie przyczyn zliberalizowano zasady dotyczące zgłoszeń zbiorów danych osobowych do rejestru Generalnego Inspektora Ochrony Danych Osobowych (GIODO), wyłączając z zakresu tego obowiązku szereg zbiorów danych („uproszczona rejestracja"). Temu celowi służyć mają również przepisy ułatwiające transfer danych do państw trzecich poprzez likwidację, w niektórych przypadkach, obowiązku uzyskiwania zgody GIODO, jak również postanowienia dotyczące tzw. uproszczonej kontroli (opisywane szerzej w dalszej części niniejszego artykułu).

Wskazane powyżej i niewątpliwie zasługujące na pozytywną ocenę zamierzenia ustawodawcy zostały jednak niestety częściowo zniweczone wprowadzeniem w ostatecznej wersji nowelizacji u.o.d.o. postanowień tworzących po stronie administratorów danych osobowych (dalej także: ADO) nowe obowiązki, w miejsce dotychczas istniejących. Przykładem jest obowiązek zgłoszenia do GIODO administratorów bezpieczeństwa informacji (dalej także: ABI) do (nowego) rejestru (art. 46b). Z punktu widzenia przedsiębiorców będących administratorami danych wątpliwości budzi również nałożenie na nich wielu nowych obowiązków w przypadku powołania, w ramach danej jednostki organizacyjnej, administratorów bezpieczeństwa informacji jako osób odpowiadających za przestrzeganie przepisów o ochronie danych osobowych (art. 36a). Z drugiej strony należy docenić wysiłki polskiego ustawodawcy, aby regulacje dotyczące tego rodzaju osób były nie tylko zgodne z już obowiązującym prawodawstwem unijnym[5], ale – co stanowi *novum* w skali Unii Europejskiej – również implementowały rozwiązania zawarte w projekcie unijnego rozporządzenia w sprawie ochrony danych osobowych, nad którym obecnie trwają prace.

3. Nowe zasady organizacji ochrony danych osobowych

Z konstrukcyjnego punktu widzenia organizacja ochrony danych osobowych przez administratorów danych może być realizowana w dwóch równoważnych modelach:

- samodzielnie przez administratora danych albo
- z udziałem administratora bezpieczeństwa informacji, powołanego przez administratora danych.

W dotychczasowym stanie prawnym funkcjonowanie ABI było regulowane jednym przepisem, tj. art. 36 ust. 3 u.o.d.o. Zgodnie z nim *„administrator wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, chyba że sam wykonuje te czynności"*. Z treści tego przepisu Generalny

[5] Dyrektywa 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 r., z późn. zm.), dalej: dyrektywa 95/46/WE.

Inspektor wywodził obowiązek wyznaczania ABI przez tych administratorów danych, którzy działają jako osoby prawne (np. spółki). Stanowisko to zostało potwierdzone w orzecznictwie sądów administracyjnych[6]. Obowiązku takiego nie mieli natomiast ci administratorzy danych, którzy byli osobami fizycznymi (np. przedsiębiorcy prowadzący jednoosobową działalność gospodarczą).

Nowelizacja u.o.d.o wprowadziła istotną zmianę w powyższym zakresie. Przepis art. 36a ust. 1 znowelizowanej ustawy stanowi bowiem, że *„administrator danych może powołać administratora bezpieczeństwa informacji"*. Równocześnie w art. 36b wyraźnie wskazano, że w przypadku niepowołania administratora bezpieczeństwa informacji zadania w zakresie zapewnienia przestrzegania przepisów o ochronie danych osobowych wykonuje administrator danych.

W świetle powyższych przepisów należy uznać, że po 1 stycznia 2015 r. każdy administrator danych (a więc również osoby prawne) może wybrać bądź model osobistego sprawowania nadzoru nad ochroną danych osobowych, bądź też utworzyć powołaną do tego specjalną strukturę, w skład której wchodzą ABI i – ewentualnie – jego zastępcy (art. 36a ust. 6).

4. Kompetencje administratora bezpieczeństwa informacji a kontrola funkcjonalna

Nowelizacja u.o.d.o. stanowi wyraz realizacji postulatu zwiększenia tzw. kontroli funkcjonalnej ochrony danych osobowych[7]. Ma się ona odbywać poprzez wprowadzenie wielu rozwiązań, które pozwalają ABI wykonywać zadania będące do tej pory wyłączną domeną Generalnego Inspektora (tzw. kontrola instytucjonalna). Ściśle związane są z tym nowe rozwiązania w postaci tzw. uproszczonej kontroli oraz uproszczonej rejestracji.

Do uproszczonej kontroli odnosi się art. 19b ust. 1 znowelizowanej ustawy. Zgodnie z tym przepisem Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Sprawdzenie to wykonywane jest u administratora danych, który powołał administratora bezpieczeństwa informacji, a jego zakres i termin określa Generalny Inspektor. Istotą kontroli uproszczonej jest więc to, że nie ma ona charakteru kontroli zewnętrznej wykonywanej przez pracowników GIODO, ale stanowi kontrolę wewnętrzną, realizowaną przez osobę powołaną przez administratora danych.

Uproszczona rejestracja jest z kolei regulowana przepisem art. 43 ust. 1a znowelizowanej u.o.d.o. Zgodnie z nim powołanie ABI i zgłoszenie go Generalnemu Inspektorowi do rejestracji skutkuje brakiem konieczności zgłaszania przez administratora danych do rejestracji zbiorów zwykłych, a więc zbiorów niezawierających danych wrażliwych, tzn. danych, których kategorie określone zostały w art. 27 u.o.d.o. Jednak, zgodnie z konstrukcją zwiększenia kontroli

[6] Wyrok Naczelnego Sądu Administracyjnego z 21 lutego 2014 r. (I OSK 2445/12).
[7] P. Fajgielski, *Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywy zmian* – dodatek do Monitora Prawniczego 2014, nr 9.

funkcjonalnej, w zakresie ww. wyłączenia – administratorzy bezpieczeństwa informacji mają (w miejsce Generalnego Inspektora) prowadzić wewnętrzne rejestry zbiorów danych.

5. Nowy status administratora bezpieczeństwa informacji

Zwiększenie znaczenia kontroli funkcjonalnej, realizowanej przez administratorów bezpieczeństwa informacji, wymagało wprowadzenia przez ustawodawcę szczególnych instrumentów, które mają im umożliwić prawidłowe wykonywanie tych zadań. Przede wszystkim wymienić należy obowiązek administratora danych zapewnienia administratorowi bezpieczeństwa informacji odpowiednich środków, jak i organizacyjnej odrębności, pozwalającej na niezależne wykonywanie przez niego określonych w ustawie zadań (art. 36a ust. 8). Przez odpowiednie środki należy rozumieć personel, pomieszczenia, sprzęt, a także inne zasoby niezbędne do wykonywania zadań. W pojęciu tym mieści się również zapewnienie utrzymania odpowiedniego poziomu wiedzy zawodowej ABI (np. poprzez zapewnienie mu możliwości uczestniczenia w różnego rodzaju szkoleniach, kursach etc.).

Z powyższym obowiązkiem ściśle związany jest wymóg, aby administrator bezpieczeństwa informacji podlegał bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych (art. 36a ust. 7). Jak się przyjmuje, takie usytuowanie administratora pozwala mu na efektywniejszą realizację zadań w zakresie ochrony danych osobowych, m.in. z uwagi na możliwość podejmowania działań władczych w stosunku do osób, które znajdują się niżej w strukturze danego podmiotu. Chodzi również o to, aby ABI wykonywał swoje zadania niezależnie i nie otrzymywał żadnych poleceń dotyczących pełnionej przez siebie funkcji.

Gwarancją należytego wykonywania zadań przez administratora bezpieczeństwa informacji jest również wymóg, aby administrator danych mógł mu powierzyć wykonywanie innych jeszcze – niż zadania z zakresu ochrony danych osobowych – obowiązków tylko wówczas, jeżeli nie naruszy to prawidłowego wykonywania tych zadań (art. 36a ust. 4). Wymóg ten należy rozumieć w ten sposób, że administrator danych powinien zagwarantować, że inne obowiązki (zawodowe) administratora bezpieczeństwa informacji będą zgodne z zadaniami tej osoby jako administratora bezpieczeństwa informacji i nie będą skutkowały konfliktem interesów. Chodzi m.in. o unikanie sytuacji określanych jako „kontrolowanie samego siebie". Niewątpliwie warunek ten, w stosunku do dotychczasowego stanu prawnego, istotnie zawęża krąg osób, które będą mogły pełnić tę funkcję.

6. Nowe zadania administratora bezpieczeństwa informacji

Nowe zadania administratorów bezpieczeństwa informacji określone zostały w art. 19b ust. 1 (działania zewnętrzne) oraz art. 36a ust. 2 pkt 1 (działania wewnętrzne) znowelizowanej ustawy. W pierwszym przypadku chodzi o dokonywanie przez administratora bezpieczeństwa informacji, na żądanie Generalnego Inspektora Ochrony Danych Osobowych, sprawdzenia u administratora danych zgodności przetwarzania danych osobowych z przepisami o ochronie

danych osobowych (uproszczona kontrola). Po dokonaniu sprawdzenia administrator bezpieczeństwa informacji przedstawia, za pośrednictwem administratora danych, sprawozdanie obejmujące badanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Elementy sprawozdania wskazane są w art. 36c znowelizowanej ustawy.

W drugiej grupie sytuacji (działania wewnętrzne) mieszczą się natomiast różne zadania, które ABI powinien wykonać w ramach struktury administratora danych. Wyróżnić należy w związku z tym dwa podstawowe rodzaje działań. Do pierwszej grupy zaliczyć trzeba zapewnienie przestrzegania przepisów o ochronie danych osobowych (art. 36a ust. 2 pkt 1). Chodzi tu o różnego rodzaju działania o charakterze wykonawczym, kontrolnym oraz opiniodawczym[8]. **W ustawie wskazano w związku z tym na takie czynności, jak: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, nadzorowanie opracowania i aktualizowania dokumentacji przetwarzania i ochrony danych osobowych oraz przestrzeganie zasad w niej określonych czy zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.**

7. Zgłoszenie administratora bezpieczeństwa informacji do rejestru Generalnego Inspektora

W przypadku wyboru modelu zarządzania ochroną danych osobowych poprzez powołanie administratora bezpieczeństwa informacji administrator danych jest zobowiązany do zgłoszenia go do rejestracji. Zgłoszenie to, z wyjątkiem „starego" administratora, powinno nastąpić w terminie 30 dni od jego powołania (art. 46b ust. 1). W ustawie wprowadzono również 14-dniowy obowiązek aktualizacyjny, dotyczący informacji objętych pierwotnym zgłoszeniem (art. 46b ust. 5).

Dokonanie zgłoszenia ABI do rejestracji w GIODO ma dwojakiego rodzaju znaczenie prawne. Po pierwsze, możliwość zażądania przez Generalnego Inspektora przeprowadzenia kontroli uproszczonej aktualizuje się dopiero po zgłoszeniu administratora do rejestracji (art. 19b ust. 1). Po drugie, zgłoszenie ABI do rejestracji jest warunkiem skorzystania przez administratora danych zbiorów ze zwolnienia z obowiązku rejestracji zbiorów danych osobowych na podstawie art. 43 ust. 1a (uproszczona rejestracja).

W noweli u.o.d.o. wprowadzono również przepisy dotyczące wykreślenia administratora bezpieczeństwa informacji z rejestru GIODO. Wyróżnić należy w związku z tym dwie grupy sytuacji. Do pierwszej zalicza się przypadki wykreślenia wskutek powiadomienia przez administratora danych o odwołaniu albo śmierci ABI (art. 46d ust. 1). Drugą grupę stanowią sytuacje, w których Generalny Inspektor dokonuje wykreślenia ABI z urzędu (art. 46d ust. 2). Tego rodzaju regulacja niewątpliwie stanowi wyraz nadania Generalnemu Inspektorowi uprawnień kontrolnych wobec administratorów bezpieczeństwa informacji.

[8] Zob. szerzej: B. Pilc, *Aktualne problemy ochrony danych osobowych,* dodatek do Monitora Prawniczego 2012, nr 7.

8. Rejestracja zbiorów danych po nowelizacji

Nowelizacja u.o.d.o. wprowadziła dwa nowe zwolnienia z obowiązku rejestracji zbiorów danych osobowych u Generalnego Inspektora. Po pierwsze, obowiązek ten w nowym stanie prawnym nie odnosi się do zbiorów, które nie są prowadzone z wykorzystaniem systemów informatycznych (art. 43 ust. 1 pkt 12). Wyjątkiem są jedynie zbiory zawierające dane, o których mowa w art. 27 ust. 1, a więc tzw. dane wrażliwe (sensytywne). Przykładem zbiorów objętych tym wyłączeniem są zbiory prowadzone w formie tradycyjnej („papierowe" kartoteki, skorowidze etc.). Po drugie, w nowelizacji ustanowiono również zwolnienie z obowiązku rejestracji w stosunku do tych administratorów danych, którzy powołali i zgłosili do rejestracji w GIODO – administratorów bezpieczeństwa informacji (art. 43 ust. 1a). Zwolnienie to, inaczej niż w przypadku art. 43 ust. 1 pkt 12, obejmuje również dane przetwarzane w systemach informatycznych, chyba że są to dane wrażliwe. W tym ostatnim przypadku nadal bowiem istnieje obowiązek zgłoszenia zbiorów do Generalnego Inspektora. Jest to wyrazem szczególnej ochrony przez ustawodawcę danych sensytywnych.

9. Transfer danych osobowych do państw trzecich – dotychczasowy stan prawny

W zakresie pojęcia przekazania danych do państwa trzeciego mieszczą się trzy grupy stanów faktycznych. Do pierwszej grupy zaliczyć należy przypadki udostępniania danych administratorowi z państwa trzeciego. Drugą grupę stanowią z kolei przypadki przekazania danych w związku z powierzeniem ich przetwarzania podmiotowi z państwa trzeciego[9]. Trzecia grupa obejmuje natomiast sytuacje transferu danych w ramach struktury organizacyjnej jednego administratora danych (np. przekaz danych do oddziału spółki znajdującego się w państwie trzecim).

Warunki legalności transferu danych ustanowione w art. 47–48 u.o.d.o. znajdują zastosowanie również do przetwarzania danych osobowych, objętych sektorowymi przepisami o ochronie danych osobowych. Przepisy tych ostatnich ustaw, np. ustawy o działalności ubezpieczeniowej, nie ustanawiają bowiem w tym zakresie odrębnych zasad.

Zgodnie z dotychczasowymi przepisami u.o.d.o., podstawową przesłanką legalizującą przekazanie danych osobowych do państwa trzeciego jest zapewnienie, aby *„państwo docelowe dało gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczpospolitej Polskiej"* (art. 47 ust. 1). W praktyce, adekwatność ochrony w państwie trzecim stwierdzana jest decyzjami Komisji Europejskiej. Najbardziej znaną z nich jest decyzja 520/2000/WE dotycząca transferu danych do Stanów Zjednoczonych (*Safe Harbour decision*). W przypadku braku decyzji tego rodzaju, przekazanie danych dopuszczalne jest na podstawie jednego z wyjątków

[9] Podmiot z państwa trzeciego ma wówczas status podmiotu, któremu powierzono przetwarzanie danych osobowych w rozumieniu art. 31 u.o.d.o.

określonych w art. 47 ust. 2 i 3 u.o.d.o. Jeżeli jednak i wówczas transfer nie jest możliwy, administrator danych powinien wystąpić o zgodę do Generalnego Inspektora, wyrażaną w formie decyzji administracyjnej (art. 48).

10. Nowe zasady transferu danych osobowych do państwa trzeciego

Znowelizowane przepisy u.o.d.o. wprowadziły istotną zmianę odnośnie do trzeciej, z wyżej wymienionych, podstaw przetwarzania danych, tj. sytuacji, w przypadku których administrator danych nie może oprzeć się na stwierdzonej – w drodze decyzji Komisji Europejskiej – adekwatności ochrony; nie może również skorzystać z jednego z wyjątków wskazanych w art. 47 ust. 2 i 3 u.o.d.o. Jak wskazuje praktyka obrotu, dotycząca również podmiotów ubezpieczeniowych, są to częste sytuacje. Jest to konsekwencją małej liczby decyzji wydanych do tej pory przez Komisję Europejską, jak również okoliczności, że ustanowione w ustawie wyjątki tworzone były przede wszystkim w interesie podmiotów danych (np. transfer danych medycznych do państwa trzeciego z uwagi na odbywane tam leczenie), a nie administratorów. Częstymi przypadkami, gdy konieczne było do tej pory wydanie zgody na transfer przez Generalnego Inspektora, były różnego rodzaju projekty IT, w ramach których dane osobowe (w tym dane ubezpieczeniowe) przechowywane były u różnego rodzaju *outsourcerów* w państwach trzecich (np. w Indiach). W dotychczasowym stanie prawnym administrator danych zawsze musiał pozyskiwać zezwolenie w takich sytuacjach. **Istotą zmiany wprowadzonej w ramach nowelizacji u.o.d.o. jest zwolnienie z konieczności uzyskania zgody w przypadku, gdy administrator danych posługuje się jednym z dwóch, wskazanych w art. 48 ust. 2 u.o.d.o., instrumentów zabezpieczenia transferowanych (przekazywanych) danych osobowych.** Chodzi w szczególności o sytuację, gdy administrator danych posługiwać się będzie *„standardowymi klauzulami umownymi”* (art. 48 ust. 2 pkt 1) lub *„wiążącymi regułami korporacyjnymi”* (art. 48 ust. 2 pkt 2).

Zakres stosowania powyższych instrumentów jest różny, w szczególności standardowe klauzule umowne mogą być wykorzystywane zarówno przy transferach w ramach danego holdingu, jak i pomiędzy podmiotami nienależącymi do danej grupy kapitałowej[10]. Zakres stosowania wiążących reguł korporacyjnych (*Binding Corporate Rules*, BCR), jest natomiast ograniczony do transferu danych osobowych pomiędzy podmiotami należącymi do tej samej grupy kapitałowej. Zasady BCR powinny przy tym obowiązywać wszystkie podmioty z grupy kapitałowej, niezależnie od miejsca prowadzenia przez nie działalności, jak i obywatelstwa osób, których dane osobowe są przetwarzane[11].

---

[10] W tym drugim przypadku konieczne jest zawieranie umów dwustronnych pomiędzy wszystkimi zainteresowanymi podmiotami, co – w przypadku większych grup kapitałowych – może stanowić pewien problem praktyczny.

[11] Zob. dokument Grupy Roboczej pt. *Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, WP 74, s.6.

Najważniejszą zaletą nowej regulacji jest ograniczenie ryzyka prawnego po stronie administratora danych. Generalny Inspektor jest bowiem związany treścią *„standardowych klauzul umownych"* zatwierdzonych przez Komisję Europejską, jak i własnymi decyzjami zatwierdzającymi *„wiążące reguły korporacyjne"*. Związanie to należy rozumieć w ten sposób, że GIODO nie może zakwestionować posłużenia się nimi jako skuteczną podstawą transferu danych.

11. Standardowe klauzule umowne jako podstawa transferu danych

W chwili obecnej obowiązują trzy decyzje Komisji Europejskiej zatwierdzające standardowe klauzule umowne, o których mowa w art. 48 ust. 2 u.o.d.o. Są to w szczególności:

- decyzja 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (klauzule „*administrator–administrator*")[12];
- decyzja 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję 2001/497/WE w zakresie alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (klauzule „*administrator–administrator*")[13];
- decyzja Komisji 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane, mającym siedzibę w państwach trzecich (klauzule „*administrator–processor*")[14].

W przypadku standardowych klauzul *„administrator–administrator"* są do wyboru dwa zestawy postanowień[15]. Zgodnie z przyjętym założeniem, obydwa zestawy postanowień mają zapewnić taki sam poziom ochrony interesów podmiotów danych, różnią je natomiast mechanizmy, które zostały ustanowione w celu zagwarantowania tej ochrony[16]. Administrator danych ma swobodę w zakresie wyboru jednego z nich. Nie wolno mu jednak zmieniać postanowień w ramach danego zestawu, nie może również łączyć poszczególnych postanowień z obydwóch zestawów[17].

Do najważniejszych zagadnień uregulowanych obydwoma zestawami standardowych klauzul zaliczyć należy zobowiązania importerów danych, a także przyznanie uprawnień podmiotom danych osobowych w związku z wykonaniem niektórych postanowień umownych. Z tą ostatnią kwestią ściśle powiązane jest określenie zasad odpowiedzialności eksportera i importera danych względem podmiotów danych.

Zgodnie z zestawem nr I klauzul umownych, importer danych jest zobowiązany do przetwarzania danych osobowych zgodnie z zasadami określonymi

---

[12] O. J. L 181/19 z 4.07.2001.
[13] O. J. L 385/19 z 29.12.2004.
[14] O. J. L 39 z 12.02.2010.
[15] Zgodnie z terminologią użytą w zatwierdzonych klauzulach, podmioty te określane są odpowiednio jako *„eksporter danych"* i *„importer danych"*.
[16] Por. przypis nr 2 preambuły do decyzji Komisji Europejskiej z dnia 27 grudnia 2004 r.
[17] Art. 1 decyzji z dnia 15 czerwca 2001 r., zmieniony decyzją z dnia 27 grudnia 2004 r.

w załączniku nr 2 i 3 do klauzul[18]. Wprowadzenie tego obowiązku ma kluczowe znaczenie dla całej konstrukcji zapewnienia odpowiedniego zabezpieczenia sposobu przetwarzania danych osobowych po dokonaniu ich transferu do państwa trzeciego. Nieco innego rodzaju mechanizmy zabezpieczenia w tym względzie wprowadzono w zestawie klauzul nr II, w tym przypadku importer danych może się bowiem zobowiązać do przetwarzania danych osobowych zgodnie z zasadami określonymi w ustawodawstwie eksportera danych[19], albo zasadami określonymi decyzją Komisji Europejskiej stwierdzającą adekwatność ochrony danych w danym państwie trzecim na podstawie art. 25 ust. 6[20], albo zgodnie z zasadami określonymi w załączniku A.

Istotne znaczenie dla kontroli sposobu przetwarzania danych osobowych w państwie trzecim ma również nałożony na importera danych obowiązek odpowiadania na zapytania eksportera danych, podmiotów danych lub właściwych organów ochrony danych osobowych odnośnie do sposobu przetwarzania przez niego danych osobowych, a także udostępniania podmiotowi danych, na jego żądanie, kopii zawartych klauzul wzorcowych[21]. Podobny charakter ma również obowiązek udostępniania swoich urządzeń przetwarzania danych lub dokumentacji w celu audytu dokonanego przez eksportera danych lub inne podmioty (*inspection body*)[22].

Treść standardowych klauzul *controller-to-processor* jest mniej rozbudowana niż w przypadku klauzul *controller-to-controller*. Wpływ na to miał zapewne fakt, że transfery tego rodzaju są traktowane jako transfery „mniejszego ryzyka" (*low risk transfer*), z uwagi na to, że dane osobowe po ich przekazaniu do państwa trzeciego są przetwarzane ściśle według wskazówek administratora danych z terytorium Unii Europejskiej.

Większość obowiązków określonych standardowymi klauzulami jest bezpośrednio związana z konstrukcją powierzenia przetwarzania danych w polskiej ustawie uregulowanej w art. 31 u.o.d.o. Zaliczyć do nich należy przede wszystkim obowiązki w zakresie zapewnienia środków techniczno-organizacyjnych przetwarzania danych[23].

12. Wiążące reguły korporacyjne jako podstawa transferu danych osobowych

Jak już wspomniano powyżej, zakres stosowania wiążących reguł korporacyjnych (*Binding Corporate Rules*, BCR) jest ograniczony do międzynarodowego transferu danych osobowych pomiędzy podmiotami należącymi do tej samej grupy kapitałowej. Transfer ten jest w szczególności dopuszczalny z uwagi na

[18] Wskazane w tych załącznikach „*mandatory data protection principles*" odpowiadają podstawowym zasadom ochrony danych osobowych określonych w dyrektywie 95/46/WE.
[19] Klauzula nr II, zestaw II, pkt h).
[20] Chodzi o sytuację, gdy została wydana decyzja o stwierdzeniu adekwatności ochrony w państwie trzecim, ale dany podmiot nie jest objęty jej zastosowaniem.
[21] Klauzula nr 5 e), zestaw I.
[22] Klauzula nr 5 d), zestaw I oraz klauzula nr II g), zestaw II.
[23] Por. klauzulę nr 4.

przyjęte w tej grupie zasady postępowania w przypadku przekazywania danych do innych państw (*codes of conduct for international transfers*). Zasady te powinny w szczególności obowiązywać wszystkie podmioty z grupy kapitałowej, niezależnie od miejsca prowadzenia przez nie działalności, jak i obywatelstwa osób, których dane osobowe są przetwarzane[24]. Zaleca się stosowanie tego instrumentu w szczególności wówczas, gdy stosowanie istniejących, tzn. zatwierdzonych decyzją Komisji Europejskiej instrumentów, jest utrudnione[25].

Zgodnie z przyjętym w nowelizacji u.o.d.o. rozwiązaniem, warunkiem możliwości posłużenia się wiążącymi regułami korporacyjnymi jest ich wcześniejsze zatwierdzenie przez Generalnego Inspektora (art. 48 ust. 3). Dotyczy to zarówno BCR opracowanych przez polskich, jak i zagranicznych administratorów danych, planujących transfer danych z terytorium Polski do państwa trzeciego.

Xawery Konarski
adwokat, starszy wspólnik w Kancelarii
Traple Konarski Podrecki i Wspólnicy

Bibliografia

Fajgielski P., *Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywy zmian*, dodatek do Monitora Prawniczego 2014, nr 9

Pilc B., *Aktualne problemy ochrony danych osobowych 2012*, dodatek do Monitora Prawniczego 2012, nr 7

Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers – dokument Grupy Roboczej, WP 74

New Principles of Personal Data Protection Organisation

The new regulations of personal data protection came into effect on 1 January 2015, which as general law are directly applicable to the processing of personal data by insurance and reinsurance undertakings as well as insurance intermediaries. These provisions shall relieve entrepreneurs processing personal data from a number of bureaucratic duties. At the same time, however, new obligations have been imposed on personal data administrators to replace the existing ones. The amendment defined the new status and new objectives for the information security administrators, who shall report directly to the organizational unit or a natural person, being a data controller. Furthermore, two additional exemptions have been introduced from the obligation to register personal data files in the Inspector General For Personal Data Protection (GIODO).

Keywords: GIODO register, information security administrator, personal data administrator, functional control, transfer of personal data to third countries.

[24] Por. dokument Grupy Roboczej pt. „*Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*", WP 74, s.6.

[25] Por. dokument WP 74, s.6.