2588/15/PL
WP 232

Opinia 2/2015 w sprawie kodeksu postępowania dotyczącego przetwarzania danych w chmurze opracowanego przez grupę roboczą C-SIG (Cloud Select Industry Group)

Przyjęta w dniu 22 września 2015 r.

Streszczenie

W niniejszej opinii Grupa Robocza Artykułu 29 (GR Art. 29) dokonała analizy projektu kodeksu postępowania w zakresie ochrony danych dla dostawców usług w chmurze (kodeksu), opracowanego przez grupę roboczą C-SIG (Cloud Select Industry Group), w której składzie znaleźli się przedstawiciele branży, który przedłożono GR Art. 29 w dniu 19 stycznia 2015 r.

GR Art. 29 docenia wysiłek podjęty przez branżę w celu opracowania projektu niniejszego kodeksu postępowania. Kodeks zapewnia ważne wytyczne dla dostawców usług w chmurze odnoszące się do mających zastosowanie zasad ochrony danych i prywatności w Europie. Przestrzeganie kodeksu postępowania przyczyni się do większej przejrzystości i pewności prawnej, dla wszystkich zaangażowanych stron.

Jednak Grupa Robocza nie może oficjalnie zatwierdzić projektu kodeksu, ponieważ nie zawsze spełnia on minimalne wymogi prawne, a wartość dodana projektu kodeksu w odniesieniu do Dyrektywy 95/46/WE i krajowego ustawodawstwa nie zawsze jest jasna. W związku z tym nadal pozostają określone istotne obawy. W niniejszej opinii dokonano analizy tych aspektów, zwracając uwagę na kwestie budzące obawy, w celu przyczynienia się do przyjęcia kodeksu, który zapewni taką wartość dodaną.

Oto kwestie, których w szczególności dotyczy opinia:
- konsekwencje przestrzegania kodeksu: przestrzeganie pomoże przedsiębiorstwom wykazać, że są odpowiedzialne/rozliczalne, ale nie uniemożliwia to organom ochrony danych realizacji ich uprawnień w zakresie egzekwowania prawa;
- zarządzanie w przypadku kodeksu: kodeks powinien odnieść się do kwestii przejścia w kierunku rozporządzenia o ochronie danych, różnicy między samooceną i certyfikacją strony trzeciej oraz uprawnień organu zarządzającego, w szczególności dotyczących mechanizmów odstraszających. Ponadto GR Art. 29 nie może być członkiem Rady Sterującej;
- odpowiedzialność: kodeks musi zapobiec przyjęciu warunków usługi, które niewłaściwie ograniczają obowiązki i zobowiązania. Kodeks musi określić (w Załączniku A), kiedy dostawca usługi w chmurze jest współ-administratorem, administratorem lub przetwarzającym oraz przydzielić zobowiązania;
- przejrzystość dotycząca lokalizacji przetwarzania danych;
- przetwarzanie szczególnych kategorii danych oraz danych szczególnie chronionych (takich jak dane finansowe czy dane dotyczące zdrowia);
- zastosowanie europejskiej definicji danych osobowych;
- wymogi dotyczące międzynarodowego przekazywania danych oraz wniosków o dostęp do danych na potrzeby egzekwowania prawa;
- środki bezpieczeństwa oraz poziom szczegółowości tych środków;
- prawo do prowadzenia audytów IT;
- odniesienie do możliwości przenoszenia danych jako kluczowego prawa użytkowników.

GR Art. 29 zachęcił postęp poczyniony przez grupę C-SIG w zakresie opracowania kodeksu i wspiera ona grupę C-SIG w jej wysiłkach na rzecz zakończenia prac nad kodeksem, z wzięciem pod uwagę uwag przedstawionych w niniejszej opinii. W związku z tym C-SIG powinna rozważyć każdą z uwag i każde z zaleceń GR Art. 29 w celu zawarcia ich w ostatecznej wersji kodeksu.

Spis treści

0. Wprowadzenie

Projekt kodeksu postępowania w zakresie ochrony danych dla dostawców usług w chmurze opracowany przez grupę roboczą C-SIG (Cloud Select Industry Group) został oficjalnie przedłożony Grupie Roboczej Artykułu 29 (GR Art. 29) 27 lutego 2014 r. GR Art. 29 podsumowała pierwszą serię uwag w piśmie przesłanym do C-SIG w czerwcu 2014 r.

Nowa wersja kodeksu biorąca pod uwagę szereg formalnych i rzeczowych uwag poczynionych w piśmie została przedłożona GR Art. 29 w dniu 21 stycznia 2015 r.

Artykuł 30 ust. 1 dyrektywy 95/46/WE stanowi że „Grupa Robocza: (…) wydaje opinie na temat kodeksów postępowania opracowywanych na poziomie wspólnotowym". W swoim dokumencie roboczym w sprawie procedury uwzględniania wspólnotowych kodeksów postępowania przyjętym 10 września 1998 r. (WP13) Grupa Robocza wyjaśniła, że gdy zostanie poproszona o wydanie takiej opinii, ustali, czy przedłożony kodeks postępowania:

- jest zgodny z dyrektywami dotyczącymi ochrony danych oraz, gdy to właściwe, krajowymi przepisami przyjętymi zgodnie z tymi dyrektywami;

- charakteryzuje się wystarczającą jakością i wewnętrzną spójnością oraz czy przewiduje wystarczającą wartość dodaną do dyrektyw lub innych właściwych przepisów prawnych dotyczących ochrony danych, szczególnie czy projekt kodeksu w wystarczającym stopniu koncentruje się na określonych kwestiach i problemach w zakresie ochrony danych w organizacji lub sektorze, do którego ma mieć zastosowanie, oraz czy oferuje wystarczająco jasne rozwiązania tych kwestii i problemów.

W tym przypadku, podczas gdy kodeks postępowania jest oczywiście przydatny dla dostawców usług w chmurze, nadal pozostają określone obawy. Niniejsza opinia odnosi się do tych aspektów, w celu przyczynienia się do przyjęcia kodeksu, który może zapewnić ważną wartość dodaną w odniesieniu do dyrektywy o ochronie danych i ustawodawstwa krajowego.

1. Rola kodeksu postępowania z perspektywy projektu rozporządzenia o ochronie danych

Podczas gdy kodeks winien przyczynić się do prawidłowego wdrożenia krajowych przepisów przyjętych zgodnie z obecną dyrektywą o ochronie danych (artykuł 27), a ocena kodeksu przez GR Art. 29 będzie oparta na obecnych ramach prawnych, niniejsza ocena również powinna być uwzględniona w świetle możliwych przepisów projektu ogólnego rozporządzenia o ochronie danych dotyczących kodeksów postępowania.

W świetle powyższego, kodeks skorzysta z dalszych określeń mechanizmów, które mogą zapewnić płynne przejście w kierunku nowego środowiska regulacyjnego.

W szczególności przyszłe ogólne rozporządzenie o ochronie danych zawiera kilka przepisów *[dotyczących sprawowania kontroli, statusu przetwarzających, kodeksów postępowania (art. 38), certyfikacji (art. 39), uprawnień i funkcji organów ochrony danych (w szczególności mechanizmu punktu kompleksowej obsługi)]*, które będą miały istotny wpływ zarówno na administratorów, jak i przetwarzających. Kodeks ustanawia Radę Sterującą, która jest zobowiązana do proponowania zmian w kodeksie oraz prowadzenia prac nad nowymi rozwiązaniami (7.1), ale mechanizmy obecnie przewidziane do tego celu są sformułowane bardzo szeroko.

Kodeks powinien wyraźnie określać, że przestrzeganie kodeksu nie powoduje, że dostawca usługi w chmurze nie będzie podlegać zmianie prawa UE. W szczególności

każdy dostawca usługi w chmurze, który będzie przestrzegał kodeksu przed wprowadzeniem do kodeksu zmian wynikających z modyfikacji ustawodawstwa UE, będzie musiał zapewnić, że zapewnia zgodność z nowym ustawodawstwem, nawet jeżeli pociąga to za sobą nowe lub sprzeczne zobowiązania w związku z kodeksem.

2. Kodeks postępowania i działania w zakresie egzekwowania prawa organów ochrony danych

Dostawcy usług w chmurze przestrzegający kodeksu niewątpliwie zamierzają wykorzystać ten środek do zmniejszenia ryzyka prowadzenia przez organy ochrony danych UE formalnych procedur egzekucyjnych (szczególnie nakładania sankcji). Taka obawa jest uzasadniona w świetle przyszłych uprawnień, które prawdopodobnie zostaną przyznane organom ochrony danych na mocy przyszłego rozporządzenia.

Przestrzeganie kodeksu nie zapewnia automatycznej ochrony przez możliwymi ingerencjami lub działaniami właściwych organów ochrony danych (lub innych organów) w czasie ich działań w zakresie nadzoru i egzekwowania prawa.

Wyjaśniając tę kwestię, GR Art. 29 zachęca dostawców usług w chmurze do przestrzegania takich kodeksów postępowania. Zapewnienie zgodności z takimi kodeksami pomoże tym dostawcom usług w chmurze wykazać, że są rozliczalni w odniesieniu do zasad ochrony danych, co będzie mieć zdecydowanie pozytywny wpływ w kontekście tych działań w zakresie nadzoru i egzekwowania prawa.

3. Zarządzanie w przypadku kodeksu

Znacząca część kodeksu poświęcona jest wdrożeniu struktury zarządzania ustanowionej z zakresem oceny stanu przestrzegania i nadzoru nad przyjęciem kodeksu przez podmioty branżowe. Aspekty te mogą bezpośrednio wpłynąć na poziom gwarancji ochrony danych dla osób, których dane dotyczą.

Po pierwsze **konieczne jest wyjaśnienie roli GR Art. 29 (7.1), ponieważ może ona nie uczestniczyć w strukturze zarządzania w przypadku kodeksu.** GR Art. 29 ustanowiono na mocy dyrektywy 95/46WE, jako organ doradczy Komisji Europejskiej, który ma (między innymi) badać każdą kwestię dotyczącą stosowania dyrektywy, aby przyczynić się w ten sposób do jej jednolitego stosowania. Jedną z głównych prerogatyw GR Art. 29 jest fakt, iż działa ona niezależnie. Z tego punktu widzenia wszelkie zaangażowanie GR Art. 29 w strukturę zarządzania, jak proponuje kodeks, wydaje się wykraczać poza zakres działania lub mandat GR Art. 29 oraz może wywołać, w ten sposób, konflikt interesów między należącymi do niej podmiotami (krajowymi organami ochrony danych) z rolą nadzorczą, jaką posiadają na poziomie krajowym wobec zaangażowanych podmiotów z branży usług w chmurze.

GR Art. 29 uznaje delikatną fazę przejścia pomiędzy ramami prawnymi, w ramach których obowiązuje kodeks. Z tego względu **wydaje się konieczne ustanowienie strategii zarządzania w okresie przejściowym, nadzorowanej przez istniejącą rzeczywistą strategię zarządzania, co pozwoli na to, aby kodeks był ważny i skutecznie przyjęty podczas okresu przejściowego i po przyjęciu nowego rozporządzenia.** W tej perspektywie w obecnym brzmieniu należy zająć się kwestią rozbieżności między czasem wdrożenia kodeksu a wejściem w życie struktury zarządzania i rozwiązać ją (np. 7.1 str. 35).

Warunki przestrzegania kodeksu opierają się albo na samoocenie albo na certyfikacjach strony trzeciej. Jednak te dwa warunki zapewniają różne poziomy zabezpieczenia. W tym względzie w kodeksie należy wyjaśnić kilka kwestii:

- **kodeks nie przewiduje wyraźnego zobowiązania do stosowania bardziej rygorystycznego podejścia przez właściwe organy[1] w przypadku samooceny.** Możliwość dokonania ponownej oceny przez właściwe organy w przypadku przestrzegania opartego na samoocenie powinna być właściwie sformułowana. W tym rozumieniu odpowiednie byłoby określenie bardziej aktywnej roli struktury zarządzania.

- W przypadku oceny 'napędzanej' certyfikacją **należy wyraźnie wskazać, że certyfikacje dostępne w przypadku przestrzegania opartego na certyfikacji muszą być typowe dla chmury** i obejmować nie tylko bezpieczeństwo, ale także wszystkie zasady ochrony danych osobowych, określone w ramach prawnych UE.

- GR Art. 29 z zadowoleniem przyjmuje fakt, że kodeks określa różne możliwe oznaczenia zgodności dla różnych schematów przestrzegania (7.4). Niemniej należy zmienić język, aby **jednoznacznie określić, że oznaczenia zgodności dla dostawców usług w chmurze dokonujących samooceny oraz oznaczenia dla certyfikowanych dostawców usług w chmurze były różne.**

I wreszcie **kodeks powinien wyjaśnić uprawnienia organu zarządzającego, szczególnie w odniesieniu do wyboru mechanizmów odstraszających**, lub warunki i procedurę, którą należy stosować w celu dokonywania, systematycznie, oceny ważności przesłanek przestrzegania, oraz decydowania o unieważnianiu wcześniej przyznanego statusu stwierdzającego przestrzeganie (7.2, 7.3, 7.4, 7.5)

4. Scenariusze konkretnych spraw dotyczących przetwarzania szczególnie chronionych kategorii danych lub przetwarzania prowadzonego dla konkretnych kategorii administratorów

Obecnie kodeks nie odnosi się do konkretnych scenariuszy w chmurze.

Nawet jeżeli oczywiście nie może to być rozwiązanie całościowe odnoszące się do wszystkich możliwych scenariuszy, **kodeks powinien odnosić się do określonych bardzo istotnych przypadków, w których dostawcy usług w chmurze oferują usługi w chmurze dedykowane przetwarzaniu danych szczególnie chronionych,** czy to w sensie prawnym (np. usługi w chmurze dla danych dotyczących zdrowia) czy w powszechnym języku (na przykład usługi w chmurze związane z usługami finansowymi). Jako że takie usługi szybko się rozwijają pod względem liczby, zakresu i rozpowszechnienia, powstają również zagrożenia ochrony danych wywołane przez przetwarzanie danych szczególnie chronionych w chmurze. Wywołują one zatem istotne obawy zarówno w przypadku profesjonalnych, jak i indywidualnych użytkowników.

Niemniej kodeks nie odnosi się do takich sytuacji, a mógłby chociaż przewidzieć, że bez szkody dla praw krajowych, takie przetwarzanie generalnie wymaga „dodatkowych zabezpieczeń".

5. Informacje na temat lokalizacji przetwarzania

Kwestię danych lokalizacyjnych podniesiono w czerwcu 2014 r. w piśmie GR Art. 29 skierowanym do grupy C-SIG dotyczącym poprzedniej wersji kodeksu. W piśmie wyraźnie wskazano, że: *„Przede wszystkim powinien być określony i wzmocniony obowiązek*

[1] Organy, które dokonują przeglądu i zatwierdzenia Deklaracji o przestrzeganiu [kodeksu] przez dostawców usług w chmurze.

informacyjny dostawców usług w chmurze. W szczególności wymagane będą konkretne i łatwo dostępne informacje dotyczące danych lokalizacyjnych, to jest bardziej konkretne informacje niż tylko kraje, w których dane będą 'przetwarzane', przetwarzane przez podprzetwarzających i/lub do których będą przekazywane oraz przez kogo dane będą przetwarzane."

Obecna wersja kodeksu nie wskazuje, ani nie zapewnia, że administrator może posiadać informacje na temat dokładnych lokalizacji, w których ma miejsce przetwarzanie[2].

Jednak w niektórych państwach członkowskich krajowe wdrożenie dyrektywy 95/46/WE obejmuje przepisy, które zobowiązują administratora do aktywnego nadzorowania, monitorowania oraz, jeżeli to konieczne, kontrolowania przetwarzania i istniejących środków bezpieczeństwa, w przypadku gdy przetwarzanie jest powierzane przetwarzającym. Administrator może wypełnić te zobowiązania tylko, jeżeli posiada dokładne informacje na temat adresu wszystkich lokalizacji, w których ma miejsce przetwarzanie prowadzone przez dostawcę usług w chmurze oraz podprzetwarzających, o ile ma miejsce. Ponadto należy z góry go informować o wszelkich zmianach tych adresów.

W celu usprawnienia procesu prawidłowego wprowadzania krajowych przepisów niektórych Państw Członkowskich, kodeks musi konkretnie odnosić się do informacji na temat adresów lokalizacji, w których ma miejsce przetwarzanie. Ze względów bezpieczeństwa przed zawarciem umowy można podać tylko ogólną lokalizację. Ten ogólny opis powinien, co najmniej, pozwolić administratorowi na określenie właściwych przepisów oraz, zawsze gdy dane są przesyłane poza UE – poinformowanie osoby, której dane dotyczą. Jak tylko zostanie podpisana umowa między administratorem a dostawcą usługi w chmurze działającym jako przetwarzający, konkretne adresy powinny być łatwo dostępne, w każdej chwili, dla administratora i organu ochrony danych.

6. Pojęcie danych osobowych

Podczas gdy kodeks odnosi się do pojęć administratorów danych i przetwarzających, do chwili obecnej nie odnosi się do pojęcia danych osobowych. Ten wybór wydaje się wywodzić z faktu, że, jak przewiduje kodeks „*dostawca usługi w chmurze działający jako przetwarzający dane generalnie nie identyfikuje danych osobowych w swojej usłudze, w szczególności gdy dostawca usługi w chmurze nie jest uprawniony na mocy umowy o świadczenie usługi do identyfikowania takich danych osobowych, lub gdy klient zastosował narzędzia takie jak szyfrowanie danych, które uniemożliwiają dostawcy usługi w chmurze identyfikowanie danych osobowych w swojej usłudze"*.

Podczas gdy takie zdanie może być istotne dla PaaS/IaaS (Platforma jako usługa/Infrastruktura jako usługa), możliwość identyfikacji często występuje w SaaS (Oprogramowanie jako usługa). Zatem zdanie należy zmienić tak, aby nie wykluczać możliwości identyfikacji przez dostawców usług w chmurze w praktyce.

Ponadto **GR Art. 29 chciałaby potwierdzić definicję danych osobowych UE, która ma być stosowana w odniesieniu do kodeksu. Takie odniesienie można wyrazić poprzez odniesienie do pojęcia anonimizacji, którego obecnie brakuje w kodeksie.** Można wskazać na wysokie standardy wymagane przez GR Art. 29 w jej opinii w sprawie anonimizacji, jak również na fakt, że **w przypadku jakiegokolwiek odniesienia do**

[2] Zgodnie z artykułem 27 ust. 1 dyrektywy 95/46/WE celem kodeksów postępowania będzie usprawnienie procesu prawidłowego wprowadzania krajowych przepisów przyjętych przez Państwa Członkowskie na mocy niniejszej dyrektywy.

pseudonimizacji może ona być uznana jako środek bezpieczeństwa, a nie jako środek, który umożliwia zwolnienie dostawców usług w chmurze lub klientów z ich zobowiązań na mocy prawa ochrony danych.

7. Międzynarodowe przekazywanie danych i wnioski o dostęp do danych na potrzeby egzekwowania prawa

Obecny projekt kodeksu jedynie powierzchownie odnosi się do kwestii egzekwowania prawa czy też rządowych wniosków o dostęp. Niemniej, jak określono w opinii 05/2012 GR Art. 29 na temat przetwarzania danych w chmurze obliczeniowej, jest to najważniejsza kwestia dotycząca ochrony danych i przetwarzania danych w chmurze obliczeniowej.

GR Art. 29 szczególnie zwraca uwagę na swoje konkretne wymogi w kwestii przekazywania lub udostępniania danych organom spoza UE, w oparciu o swoją interpretację proponowanego artykułu 43A ogólnego rozporządzenia o ochronie danych. Zawarcie takich wymogów w projekcie kodeksu będzie również zgodne z jej oczekiwaniami, aby kodeks postępowania wykraczał poza zwykłą zgodność z prawem[3].

Ponadto, jak opisano w poprzednich opiniach[4], kodeks powinien określać, że:

- przetwarzający informuje administratora danych o jakichkolwiek prawnie wiążących wnioskach o ujawnienie danych osobowych ze strony organów ścigania, chyba że powiadomienie o takim wniosku jest zabronione,

- oraz **w każdym przypadku przekazywanie danych osobowych przez przetwarzającego organowi publicznemu nie może mieć charakteru masowego, nie może być nieproporcjonalne ani nieprzemyślane w sposób, który wykracza ponad to, co jest niezbędne w demokratycznym społeczeństwie.**

I wreszcie dostawcom usług w chmurze należy przypomnieć, że również w przypadku międzynarodowego przekazywania danych powinni postępować ściśle zgodnie z instrukcjami otrzymanymi od klienta. Dostawcę usług w chmurze można przestać uważać za przetwarzającego, ze wszystkimi tego konsekwencjami szczególnie pod względem odpowiedzialności, w przypadkach gdy działania podejmowane przez dostawcę usług w chmurze znacznie przekraczają normalne możliwości przetwarzającego dane w świetle rzekomego braku jego niezależności w odniesieniu do instrukcji administratora. Może to mieć miejsce na przykład, gdy dostawcy usług w chmurze niezależnie organizują międzynarodowe przekazywanie danych w celu odpowiedzi na wniosek organu ds. egzekwowania prawa lub bezpieczeństwa państwa, nie dążąc do zaangażowania właściwych administratorów[5].

8. Odpowiedzialność

Kodeks nie omawia wystarczająco kwestii systemu odpowiedzialności mającego zastosowanie do stron w przypadku naruszenia ich zobowiązań w zakresie ochrony danych.

W opinii GR Art. 29 05/2012 na temat przetwarzania danych w chmurze obliczeniowej podkreślono, że ważne jest wyjaśnienie roli każdej ze stron w celu określenia ich konkretnych

[3] Patrz WP 13.
[4] Patrz WP 204 rew.01 – Dokument wyjaśniający w sprawie wiążących reguł korporacyjnych dla przetwarzających
[5] Patrz str. 11 opinii 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication (SWIFT)

zobowiązań w odniesieniu do ustawodawstwa w zakresie ochrony danych oraz przypisania odpowiedzialności za możliwe naruszenie tych przepisów. Uczynienie tego pozwoli uniknąć ewentualnych luk, z powodu których niektóre zobowiązania lub prawa wynikające z ustawodawstwa o ochronie danych nie będą wykonywane przez żadną ze stron[6]. Ponadto proponowany artykuł 26 ust. 4 przyszłego ogólnego rozporządzenia o ochronie danych[7] powinien pomóc dostawcom usług w chmurze, zapewniając większą jasność co do ich zobowiązań i odpowiedzialności w takich przypadkach. W tym względzie **kodeks musi zapobiec przyjmowaniu warunków usług, które są niekorzystne dla klientów z powodu nieodpowiedniego ograniczenia zobowiązań i odpowiedzialności dostawców usług w chmurze oraz ograniczenia praw klientów[8].**

Rozdzielenie zobowiązań pomiędzy strony komercyjne jest przedmiotem obaw osób zawsze, gdy może mieć to na nich negatywny wpływ. Zatem kodeks musi określić, że niezależnie od tego jak będzie wyglądał podział zobowiązań, nie może on pozbawiać osób ich praw ani możliwości uzyskania wyrównania ewentualnej poniesionej przez nie szkody. W szczególności w przypadku współadministrowania należy wyraźnie rozdzielić różne role i zobowiązania dotyczące przetwarzania danych między dostawcę usługi w chmurze a klienta, aby ułatwić realizację swoich praw przez osoby, których dane dotyczą. Ponadto system odpowiedzialności mający zastosowanie odpowiednio do klientów i dostawców usług w chmurze, jak również do ewentualnych podprzetwarzajacych, dodatkowo do umowy o świadczenie usług, musi być określony wyraźniej (np. jak wskazano w punkcie 5.8). **Ponadto Załącznik C powinien określić, jakimi obszarami przetwarzania zarządza dostawca usługi w chmurze jako współadministrator, administrator lub przetwarzający, oraz powinien zapewnić informacje na temat rozdzielenia odpowiedzialności między dostawcę usługi w chmurze a jego klienta.**

Ponadto artykuł 77 przyszłego rozporządzenia o ochronie danych przewiduje domniemane współadministrowanie oraz kilka systemów odpowiedzialności, przy czym administrator i przetwarzający muszą być zwolnieni z tej odpowiedzialności, jeżeli wykażą, że nie są odpowiedzialni za szkodę. Takie domniemanie odpowiedzialności może w związku z tym być obalone przez każdy podmiot zaangażowany w operację przetwarzania, bez szkody dla roszczeń regresowych administratora wobec przetwarzającego w przypadku, gdy ten ostatni nie może udowodnić, że nie jest odpowiedzialny za określoną szkodę. Ten projekt ram jest w rzeczywistości zgodny ze stanowiskiem zajętym przez GR Art. 29 w szczególności w jej opinii na temat przetwarzania danych w chmurze obliczeniowej i podprzetwarzania (WP196, str. 9-10). W opinii tej położono nacisk na potrzebę jasnego rozdzielenia odpowiedzialności pomiędzy różne podmioty oraz potrzebę wprowadzenia konkretnych zabezpieczeń również w odniesieniu do osób, których dane dotyczą. Takimi zabezpieczeniami mogą mianowicie być prawa beneficjenta-strony trzeciej sformułowane na wzór tych ze standardowych klauzul umownych stosowanych do relacji administratora do przetwarzającego.

GR Art. 29 zaleca rozszerzenie tej części kodeksu, ze zwróceniem szczególnej uwagi na rozpatrywanie skarg/wniosków osób, których dane dotyczą (5.8) oraz potrzebę prowadzenia w tym celu przez dostawcę usługi w chmurze współpracy z klientami.

---

[6] Jest to tym ważniejsze, zważywszy że mogą być różne poziomy sprawowania kontroli i sytuacje, w których dostawcę usług w chmurze można uznać albo za współadministratora danych albo za samego administratora danych w zależności od konkretnych okoliczności.

[7] Które przewiduje, że przetwarzającego, który przetwarza dane osobowe inne niż wskazał administrator, należy uznać za administratora

[8] Patrz Opinia EIOD w sprawie komunikatu Komisji dotyczącego "Uwolnienia potencjału przetwarzania danych w chmurze obliczeniowej w Europie", 6 listopada 2012 r., str. 5.

Postanowienia kodeksu zapewniające konkretne korzyści osobom można również określić jako bezpośrednio przez nie wykonalne; należy również określić, że systemem odpowiedzialności mającym zastosowanie wobec stron może być wyłącznie system państw członkowskich UE.

9. Bezpieczeństwo

Ochrona danych osobowych obejmuje także zapewnienie bezpieczeństwa IT. GR Art. 29 zaleca wzięcie tego pod uwagę w strukturze i treści kodeksu, gdzie aspekty bezpieczeństwa mają nie być najważniejsze w ochronie danych osobowych, ale mają stanowić jej niezbędną część.

Przetwarzający dane musi działać „wyłącznie na polecenie administratora danych" (art. 17 ust. 3) i w związku z tym powinien ukształtować swoją rolę jako zwykły środek do osiągnięcia celu będący w rękach administratora, bez angażowania się w semantykę przetwarzania i bez marginesu swobody dla żadnego rodzaju dalszego przetwarzania[9]. Zasada ta powinna być odzwierciedlona w interfejsach technicznych, poprzez które odbywa się interakcja administratorów i dostawcy usługi w chmurze jako przetwarzającego. W związku z tym role i zobowiązania powinny być wyraźnie zdefiniowane w kodeksie.

Ponadto środki bezpieczeństwa i możliwości prowadzenia audytu powinny być zorganizowane w taki sposób, aby brać pod uwagę cechy charakterystyczne i zagrożenia nierozerwalnie związane z różnymi pojawiającymi się paradygmatami dla usług w chmurze, mianowicie IaaS (Infrastruktura jako usługa), PaaS (Platforma jako usługa) oraz SaaS (Oprogramowanie jako usługa), gdzie przewidziany jest rosnący poziom zagrożenia prywatności ze względu na nieodłączne cechy charakterystyczne.

Kodeks stanowi, że „*kluczowym celem w zakresie bezpieczeństwa jest to, aby dostawca usługi w chmurze umożliwił klientowi dokonanie oceny zagrożenia bezpieczeństwa oraz oceny wpływu na ochronę danych*". Jest to rzeczywiście niezbędne dla administratora (klienta), aby wprowadzić środki bezpieczeństwa, które, zgodnie z art. 17 dyrektywy, są „*odpowiednie do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną".*

W tym celu rzeczywiście fundamentalne znaczenie ma to, aby dostawca usługi w chmurze zapewnił klientowi „*wystarczający poziom szczegółowości środków bezpieczeństwa wdrożonych przez dostawcę usługi w chmurze".* Choć uzupełnieniem tego powinien być także **wystarczający poziom informacji na temat zagrożeń i słabych stron usługi oraz infrastruktury dostawcy usługi w chmurze, a także na temat decyzji w zakresie zarządzania ryzykiem podejmowanych przez dostawcę usługi w chmurze.** Jeżeli nie ma to miejsca, podstawy do prowadzenia przez klienta własnego zarządzania ryzykiem dotyczącym ochrony danych nie będą odpowiednie. Niemniej przy zapewnianiu takich informacji należy uwzględnić potrzeby dostawcy usługi w chmurze w zakresie poufności ze względów bezpieczeństwa i względów biznesowych.

Kodeks nakłada także na dostawcę usługi w chmurze obowiązek przeprowadzenia oceny ryzyka „*aby zapewnić, że dla osoby, której dane dotyczą, zagwarantowane jest prawo do ochrony danych osobowych".* **Dostawca usługi w chmurze powinien uwzględnić**

[9] Jednakże zgodnie z opinię 2/2010 GR Art. 29 w sprawie pojęć „administrator danych" i „przetwarzający" „Przekazanie uprawnień może wiązać się jednak z pewnym stopniem swobody uznania w odniesieniu do możliwie najlepszego sposobu działania w interesie administratora danych, umożliwiając przetwarzającemu dokonanie wyboru najbardziej odpowiednich środków technicznych i organizacyjnych".

ustanowienie różnych poziomów ochrony w zależności od „*przetwarzania i charakteru danych objętych ochroną*" oraz ich publiczne ogłoszenie przy oferowaniu swoich usług. Zmniejszy to brak wystarczających informacji od dostawcy usługi w chmurze dla potencjalnego klienta na temat zagrożeń, słabych stron i ogólnego zarządzania ryzykiem.

GR Art. 29 uznaje i przyjmuje z zadowoleniem fakt istnienia zestawu minimalnych celów w zakresie bezpieczeństwa. Niemniej są one sformułowane ogólnie i tym samym, w przypadku samooceny bezpieczeństwa mogą nie zapewnić wystarczających gwarancji solidnego zarządzania bezpieczeństwem. Te cele oraz ich sformułowanie mogą być dalej porównane z tymi istniejącymi w normach bezpieczeństwa i najlepszych praktykach. Na przykład, nawet jeżeli podejście zarządzania ryzykiem jest zawarte w kodeksie, brak jest wyraźnego celu w zakresie bezpieczeństwa, który odnosiłby się do niego. GR Art. 29 zaleca ponadto ujęcie tych celów w zakresie bezpieczeństwa w kontekście szerszego zestawu celów dotyczących bezpieczeństwa.

Za możliwe rozwiązania alternatywne uznać można także „materiały potwierdzające" (ang. demonstration keys), choć nie są one równoważne i dają inny poziom gwarancji. Na przykład w punkcie 6.1 napisano, że „*dostawcy usług w chmurze określą istniejące środki techniczne, fizyczne i organizacyjne w celu ochrony danych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, nieuprawnionym wykorzystaniem, modyfikacją, ujawnieniem lub dostępem oraz przed innymi nielegalnymi formami przetwarzania"*. Zapewnienie „*kopii certyfikatu lub atestu stanowiącego dowód skutecznego zakończenia niezależnego audytu przez stronę trzecią"* niekoniecznie zawiera te informacje.

I wreszcie GR Art. 29 chciałaby podkreślić, że norma ISO/IEC 27018 to katalog najlepszych praktyk dla dostawców usług w chmurze działających jako przetwarzający. Opisuje ona listę kontroli mających poprawić ochronę prywatności. Norma ta jest tylko dobrym zbiorem nieobowiązkowych, niewyczerpujących i nie maksymalistycznych kontroli, które można wprowadzić. Zatem ISO/IEC 27018 nie powstała w celu wykorzystania jej jako samodzielnego dokumentu do certyfikacji. Może być stosowana w połączeniu z normą ISO/IEC 27001, która umożliwia certyfikację. ISO/IEC 27001 nie bierze pod uwagę cech charakterystycznych ochrony prywatności, takich jak wpływ na osoby, ale zapewnia wysoki poziom ochrony informacji w interesie organizacji. Dodanie dobrych praktyk opartych na ISO/IEC 27018 może zatem pomóc zapewnić, że prywatność będzie bardziej brana pod uwagę, ale nie jest dowodem na to, że uwzględniane są zagrożenia prywatności. Najlepiej by było, gdyby ISO/IEC 27018 była stosowana tylko po ocenie zagrożeń prywatności osób, których sprawa dotyczy, aby traktować je w proporcjonalny sposób. Na chwilę obecną żadna z opublikowanych norm nie opisuje sposobu realizacji tego procesu. Trwające prace w ISO (Międzynarodowej Organizacji Normalizacyjnej) mogą pomóc w wypełnieniu tej luki w ciągu najbliższych kilku lat.

10. Prawo do audytu

Co do zasady, prawo do audytu powinno być generalnie zagwarantowane i nie powinno być ściśle ograniczone do sytuacji, w której dostawca usługi w chmurze nie został certyfikowany przez niezależny organ. W rzeczywistości dyrektywa 95/46/WE przewiduje, że:

- na administratorze danych spoczywa obowiązek zapewnienia przestrzegania wszystkich wymogów jakości danych z art. 6 ust. 1 (art. 6 ust. 2),

- przetwarzający działa wyłącznie na polecenie administratora danych (art. 16 i art. 17 ust. 3).

Obowiązek nadzoru spoczywający na administratorze jest przesłanką prawa, które jest im przy przyznane, aby prawidłowo prowadzić kontrolę działań wprowadzonych przez

przetwarzającego. Prawo to powinno być realizowanego przez każdego administratora, niezależnie od jego siły gospodarczej, umiejętności i możliwości technicznych.

Oznacza to, że jako warunek wstępny skutecznego nadzoru nad przetwarzaniem danych przez dostawcę usługi w chmurze podmioty z branży muszą przestrzegać w swojej działalności szeregu 'kluczowych wskaźników wyników' (KPI). Administrator może być skutecznie rozliczalny, jeżeli może wykazać w wymierny sposób, że wypełnia zobowiązania UE w zakresie ochrony danych. Jeżeli brak jest powiązania między obowiązkiem rozliczalności administratorów danych a mierzalnością przetwarzania wprowadzoną przez dostawców usług w chmurze na podstawie instrukcji otrzymanych przez administratora (a jest to szczególnie istotne, gdy istnieje ogromny brak równowagi między tymi dwoma aspektami), obowiązek rozliczalności nie może być odpowiednio spełniony.

Następnie może być określone prawo do audytu w celu uwzględnienia różnych faz przetwarzania oraz zajęcia się cechami charakterystycznymi zagrożeń związanych z przetwarzaniem lub charakterem przetwarzanych danych, oraz może sięgać od prawa przeprowadzenia audytu lokalizacji serwerów, w których dane są przetwarzane i przechowywane, po prawo do przeprowadzenia audytu logiki (algorytmów) stosowanej podczas różnych kroków przewidzianych dla całego przetwarzania, po prawo do przeprowadzenia audytu środków bezpieczeństwa wprowadzonych przez przetwarzającego.

GR Art. 29 z aprobatą zwraca uwagę na wdrożenie norm dla przetwarzania danych w chmurze obliczeniowej, szczególnie związanych z interoperacyjnością danych, ich przenoszalnością oraz bezpieczeństwem, oraz zachęca branżę do przyjęcia uzgodnionych na poziomie międzynarodowym rozwiązań dla tych obszarów jako warunek wstępny przestrzegania kodeksu. Ponadto należy podjąć wszelkie możliwe wysiłki w celu wdrożenia interfejsów między systemami przetwarzających a aplikacją administratora, tak by ułatwić sprawną realizację możliwości audytowych przez dostawców usług w chmurze.

Możliwości te powinny być wyraźnie odzwierciedlone w kodeksie, który powinien obejmować przypadki, w których role i zobowiązania są określone wraz z możliwościami audytowymi, które dostawcy usług w chmurze udostępnią.

11.Prawa użytkownika

Obecnie większość dostawców usług w chmurze nie stosuje standardowych formatów danych i interfejsów usługi ułatwiających interoperacyjność oraz przenoszalność między różnymi dostawcami usług w chmurze. Jeżeli klient usługi w chmurze postanowi przenieść się od jednego dostawcy usługi w chmurze do innego, brak interoperacyjności może uniemożliwić albo co najmniej utrudnić przekazanie danych (osobowych) klienta do nowego dostawcy usługi w chmurze[10]. To samo dotyczy usług, które klient rozwinął na platformie oferowanej przez pierwotnego dostawcę usługi w chmurze (PaaS).

Podczas gdy punkt 5.8 kodeksu przewiduje współpracę w dobrej wierze dostawcy usługi w chmurze w celu ochrony praw osoby, której dane dotyczą, prawa te są wymienione tylko jako: prawo dostępu do ich danych osobowych, do ich poprawiania i usunięcia w sposób terminowy i skuteczny. Jedyne odniesienie do kwestii przenoszalności danych zawarte jest obecnie w formularzu przejrzystości w Załączniku A. Jako że kodeks ma na celu pomóc „przewidzieć reformę ochrony danych", **odniesienie do przenoszalności przyczyniłoby się do trwałości kodeksu.**

[10] Znane jest to również jako tzw. uzależnienie od dostawcy (ang. vendor lock-in)

I wreszcie, jeżeli chodzi o relację z osobą, której dane dotyczą, GR Art. 29 zwraca uwagę grupy C-SIG na artykuł 10 dyrektywy[11] 95/46/WE.

W rezultacie, **kodeks skorzysta na dodaniu klauzuli, która wyraźnie przypomni dostawcy usługi w chmurze o tym, że powinien, w zależności od kontekstu, albo zapewnić odpowiednie informacje osobie, której dane dotyczą, albo współpracować w dobrej wierze ze swoim klientem, aby umożliwić mu odpowiednie informowanie osób, których dane dotyczą.**

12. Zakończenie

GR Art. 29 zachęcił postęp poczyniony przez grupę C-SIG w zakresie opracowania kodeksu i wspiera ona grupę C-SIG w jej wysiłkach na rzecz zakończenia prac nad kodeksem, z wzięciem pod uwagę uwag przedstawionych w niniejszej opinii i w poprzedniej korespondencji.

GR Art. 29 uznaje wartość, jaką taki kodeks może zapewnić branży usług przetwarzania danych w chmurze oraz zapewnia pomoc administratorom danych w ocenie dostawców usług w chmurze, a w szczególności produktu lub usługi w chmurze. Jednak w obecnej formie kodeks nadal zawiera szereg znaczących luk, którymi należy się zająć przed zakończeniem prac nad kodeksem.

W związku z tym GR Art. 29 zaleca, aby grupa C-SIG rozważyła każdą z uwag i każde z zaleceń GR Art. 29 w celu zawarcia ich w ostatecznej wersji kodeksu.

[11] Państwa Członkowskie zapewniają, aby administrator danych lub jego przedstawiciel dostarczył osobie, której dane dotyczą, co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona takie informacje:
a) tożsamość administratora i ewentualnie jego przedstawiciela;
b) cele przetwarzania danych;
c) wszelkie dalsze informacje, jak np.:
- odbiorcy lub kategorie odbierających dane,
- czy odpowiedzi na pytania są obowiązkowe czy dobrowolne, jak również możliwe konsekwencje nieudzielenia odpowiedzi;
- istnienie prawa wglądu do swoich danych oraz ich sprostowania,
o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą.