

PROTOKÓŁ z XLIII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 16 grudnia 2022 roku, o godzinie 13:00 w formie wideokonferencji.

Omówienie projektu Data Act - Pan Michał Kanownik oraz ekspert Rady Pan Jarosław Mojsiejuk z udziałem przedstawicieli Departamentu Zarządzania Danymi w KPRM.

Pan Jarosław Mojsiejuk rozpoczął od wskazania, że projekt Data Act to rozporządzenie unijne, które ma regulować najważniejsze kwestie związane z przenoszeniem danych zwłaszcza danych chmurowych oraz różnego rodzaju innych materii. Odniósł się do trzech głównych problemów, którymi są: współdzielenie danych, przenoszenie danych z chmury do chmury (cloud switching), transfer danych poza EOG.

Projekt Data Act jest postrzegany przez autorów wystąpienia jako kropla w tsunami legislacyjnym UE. Wymieniono istniejące i względnie nowe akty: Cybersecurity Act, DMA, DSA, DGA, NIS 2, DORA, CER, Projekt rozporządzenia dot. AI.

Zauważono istnienie problemu z Data Sharing – instytucją współdzielenia danych, która pojawia się w kilku miejscach, zwłaszcza w kontekście potrzeby wzmocnienia zapisów chroniących tajemnice handlowe czy tajemnice przedsiębiorstwa (również własności intelektualnej).

Zwrócono uwagę na konieczność wyraźnego wyróżnienia zakresu odpowiedzialności dostawców infrastruktury, na której odbywa się przetwarzanie danych (np. dostawców chmury).

Wspomniano o problemach związanych z przenoszeniem chmury do chmury, czyli Cloud Switching:

- Odpowiedzialność za możliwość przeniesienia nałożona na dostawcę chmury – brak wymagań wobec użytkowników i nowych dostawców
- Projektodawca zakłada tzw. równowagę funkcjonalną przy przenoszeniu. Jest to określenie niejasne i ogranicza innowacyjność („zamraża pewien status quo standardów”).
- Wymaga się ograniczonego okresu zakończenia usługi.

Ww. regulacje są nierealistyczne w przypadku złożonych aplikacji. Brakuje dookreślonych ścieżek postępowania w przypadku, gdy pojawią się obiektywne trudności.

Przenoszenie się użytkownika pomiędzy dostawcami usług zostało opisane w motywie (72) i nast., definicji art. 2.

Brak jest wymogu zachowania równowagi funkcjonalnej dla rozwiązań typu PaaS i SaaS. Motyw (72) wskazuje, że równowaga funkcjonalna pomiędzy dostawcami usług ma zachodzić dla funkcjonalności oferowanych przez obu dostawców. Proces ten ma być darmowy, tzn. dostawcy w porozumieniu wyeliminują wszelkie przeszkody oraz zagwarantują, że wszystko odbędzie się w sposób bezpieczny, efektywny i zakończony

sukcesem. Zapewniona zostanie u nowego dostawcy taka sama wydajność procesu przy zachowaniu tego samego poziomu bezpieczeństwa, odporności i jakości serwisu u dotychczasowego dostawcy. Motyw (72a) wskazuje, że dowód nieprzenoszalności jest także nałożony na aktualnego dostawcę.

Następnie wskazano, że odpowiedzialność spoczywa wyłącznie na dotychczasowym dostawcy, a jest to proces, w którym uczestniczą także użytkownik czy powierzający przetwarzanie danych w chmurze i drugi dostawca. Aktualny dostawca powinien monitorować równowagę funkcjonalną wszelkich innych dostawców. Według motywu (72b) zabronione będzie nakładanie jakichkolwiek kosztów, w tym kosztów suportu technicznego.

W przekonaniu autorów prezentacji te mechanizmy doprowadzą do tworzenia podwójnego systemu usług typu data processing services. Pierwszy system to usługi wystandaryzowane i bardzo rzadko podlegające zmianom. Drugi system to usługi z ogromnym udziałem innowacyjnych zmian, dodatkowych funkcjonalności i o bardzo wysokich parametrach przetwarzania, pozwalające łatwo wykazać brak możliwości przeniesienia do innego dostawcy.

Zauważono, że mogą powstać usługi gorsze i droższe, tzn. wystandaryzowane i które oznaczają niemożliwość nałożenia dodatkowych opłat za migrację albo usługi oparte o innowacyjność, które są nieprzenoszalne – klient będzie miał świadomość, że jest to ryzyko polegające na vendor lock-in. Wymóg przenoszalności to konieczność trzymania się sztywnych reguł, norm i specyfikacji zapisanych wg art. 29. Nieznany jest czas powstania standardu, częstotliwości ani procesu aktualizowania zawartych w nim norm, co rodzi wątpliwości użytkowników i dostawców.

Kolejnym zarzutem są nierealistyczne terminy przenoszenia. 30-dniowe terminy są nie do zrealizowania w przypadku bardziej skomplikowanych usług. Właściwym rozwiązaniem może być przynajmniej 90-dniowy termin oraz zapis możliwości uzgodnienia terminu pomiędzy użytkownikiem a dostawcą.

Wskazane zostało, że standardem usługi chmurowej jest samoobsługa i samodzielny wybór usług. Dostawca nie ma wpływu na wybór użytkownika.

Ograniczenie innowacyjności nie będzie dotyczyło dostawców, ale firm korzystających z modelu B2B2B lub B2B2C. Coraz więcej firm to oferenci rozwiązań chmurowych (zwłaszcza dedykowanej chmury).

Kolejną poruszoną kwestią był problem transferu danych osobowych poza granice EOG, który jest określony w RODO. RODO przewiduje trzy mechanizmy dopuszczalnego transferu. W przypadku danych nieosobowych jedynie art. 27 ust. 1 wskazuje: „*Transfer jest niedopuszczalny poza UE, jeśli może to stać w sprzeczności z prawem unijnym lub prawem kraju członkowskiego. Zadanie przeciwdziałania od strony kontraktowej, prawnej, organizacyjnej i technicznej leży po stronie dostawcy usług przetwarzania*”. Stwierdzono, że jest to niezrozumiałe, ponieważ bez Data Act można przyjąć wykładnię argumentum ad

maiori to minus „jeżeli można więcej, to można i mniej”. Zauważono, że kwestie dot. transferu danych nieosobowych wewnątrz UE reguluje odrębne rozporządzenie.

Jeśli dostawca traktuje wszystkie dane jako potencjalnie dane osobowe i w odpowiedni sposób je chroni, to może to nie spełniać wymagań art. 27 ust. 1. Należy wprowadzić zapis o odpowiedzialności „data holder” za ocenę wypełniania wymogów art. 27 lub zapis, że dostawca usługi otrzymał informacje, że będą przetwarzane dane objęte dodatkowymi wymaganiami. Dostawcy usług stosują techniki szyfrowania wg wyboru klienta.

Stosowanie restrykcji w transferze danych nieosobowych na poziomie równym lub wyższym niż dla danych osobowych jest niewłaściwym sposobem podejścia do tej kwestii. O ile żądanie dostępu do danych przez państwa trzecie może mieć zastosowanie, to restrykcje transferu są wątpliwe. Wystarczające byłoby wskazanie dodatkowych środków zabezpieczających dane wskazujących na konieczność ochrony. Zwrócono uwagę, że wpłynie to na ograniczenie działalności gospodarczej, w tym na obniżenie wartości europejskich firm. Część danych nieosobowych firmy europejskiej nie będzie, bądź nie jest transferowalna poza granice UE. Wyjście europejskiej firmy poza granice UE będzie miało dodatkowy i natychmiastowy koszt, a największe koszty poniosą europejscy dostawcy.

Stwierdzone zostało, że Data Act zmierza w kierunku restrykcyjności transferów. Nie odpowiada to ryzyku związanemu z przetwarzaniem takich danych. Data Act nie ma opisanych mechanizmów, które pozwalają na szybką ocenę możliwości transferu.

Data Act obarcza odpowiedzialnością za ocenę transferów dostawców usług przetwarzania. Pomija fakt, że to nie oni są właścicielami danych, ani nie wiedzą jakie dane zostały do nich przekazane przez użytkowników usługi. W Data Act wybrzmiewa dążenie do europejskiej autarkii w obszarze technologii cyfrowych. W obecnym stanie i w perspektywie następnych dziesięcioleci jest to niemożliwe do zrealizowania.

Zapisy projektu nie uwzględniają, że:

1. Czas i koszt związany z przejściem klienta z jednej chmury do innego usługodawcy są zmienne i zależne od wielu czynników.
2. W chmurze dostawca nie kontroluje danych zabezpieczonych za pomocą silnej kryptografii.
3. Dostawcy usług nie są w stanie zrealizować całego procesu przełączania lub udzielić gwarancji w odniesieniu do czasu zmiany.

Dostawcy nie powinni być zobowiązani do udostępniania własnych wygenerowanych przez siebie danych i informacji dotyczących użytkownika, wydajności. Nie mogą być zobowiązani do udostępniania ich konkurencji.

Podsumowując wskazane zostało, że:

- Możliwe jest tworzenie standardów interoperacyjności na podstawie już istniejących przepisów;

- Normy dotyczące interoperacyjności danych nie powinny być obowiązkowe we wszystkich przypadkach, ponieważ to szkodzi innowacyjności;
- Zgłaszane przez prezydencję francuską standardy dot. EUCS są nie do przyjęcia i zmierzają do dyskryminacji działających w Polsce dostawców chmury;
- Jest problem z wypracowywaniem standardów w organizacjach: Gaia X, European Alliance for industrial data - prace się toczą bez udziału polskich firm.
- Zwrócono uwagę, że zlecona przez KPRM praca fundacji Instrat prześlizguje się po temacie interoperacyjności czy przenoszalności danych;
- Projekt Data Act nie uwzględnił elementów dotyczących przenoszenia i transferu danych;
- Znaczna część procesów znajduje się pod kontrolą klientów lub dostawcy docelowego;
- Porównywalność tych samych rodzajów usług jest bardzo trudna;
- Zakaz transferu danych poza EOG nie powinien dotyczyć dojrzałych demokracji (Kanada, USA, Australia, Nowa Zelandia, Japonia, Wielka Brytania);
- EROD nie widzi przeszkód w transferze danych osobowych z UE do Rosji ze względu na „ekonomiczne i historyczne bliskie związki niektórych państw UE z Rosją”;
- Zwrócono uwagę, że wszystkie operacje czy podstawowe instytucje Data Act będą rodziły bardzo istotne koszty.

Pan Michał Kanownik dodał, że prezydencja czeska wprowadziła pewne modyfikacje projektu wyjściowego Data Act, które nie zmierzają w dobrym kierunku. W projekcie trzeba pogodzić interesy otwartości danych, a z drugiej strony bardzo restrykcyjne zapisy unijne odnośnie ochrony danych. Należy także mieć na uwadze otwartość relacji gospodarczych pomiędzy UE a Stanami Zjednoczonymi. Dochodzi do nakładania się różnego rodzaju interesów, choćby francuskie podejście suwerennościowe do cyfrowego europejskiego rynku. Za niepokojący uznano fakt, iż przez KE nie przebiły się uwagi, które składał biznes na etapie konsultacji do ww. projektu.

Zaproponowano, aby na bazie przedstawionych uwag Rada przygotowała stanowisko wzmacniające polski rząd w negocjacjach, z uwagi na to, że omawiany akt ma kluczowe znaczenie dla przyszłości transferu danych.

Omówienie ostatniej wersji projektu ustawy o przekształceniu Centralnego Ośrodka Informatyki w Agencję Informatyzacji – Pan Wiceprzewodniczący Dariusz Milka.

Pan Wiceprzewodniczący Dariusz Milka wskazał, że w ramach konsultacji projektu ww. ustawy z Panem Ministrem Januszem Cieszyńskim zostały zgłoszone uwagi. Niektóre z uwag dotyczyły wprost zapisów w projekcie ustawy, zaś inne odnosiły się do interpretacji/rozumienia tych zapisów. W konsekwencji spotkania zainteresowanych tematyką członków Rady z udziałem Pana Ministra pojawiła się nowa propozycja ww. ustawy w której szereg spraw, będących przedmiotem rozmowy, zostało dopracowanych w formie konkretnych zapisów i modyfikacji artykułów, bądź też bardziej szczegółowo zdefiniowana w obszarach dotyczących zadań, uprawnień oraz zakresu działania Agencji Informatyzacji.

W stosunku do poprzedniej wersji projektu ustawy usunięty został zapis, że prezesem Agencji Informatyzacji zostaje automatycznie Dyrektor Centralnego Ośrodka Informatyki – prezes Agencji zostanie wyłoniony w drodze konkursu. Wiceprezesów na okres przejściowy wyznacza się spośród pracowników COI. Takie działanie oceniono jako rozsądne, ze względu na zapewnienie płynności przebiegu procesu, a sam proces opisany w projekcie ustawy dotyczący przejmowania zobowiązań oraz wkraczania w nowe obszary, w których Agencja ma funkcjonować, nie będzie szybkim i prostym zadaniem.

Co również wydaje się istotne, w poprzedniej wersji projektu ustawy znalazł się zapis, że statut Agencji miał nadać prezes, co wydawało się zbyt daleko idące i w obecnym zapisie zostało wyraźnie uregulowane, że *minister właściwy do spraw informatyzacji nadaje, w drodze zarządzenia, statut Agencji, mając na uwadze zakres jej zadań oraz konieczność zapewnienia sprawnej i efektywnej ich realizacji*, co zostało ocenione jako rozsądne rozwiązanie. Mając na uwadze, że Agencja ma być instytucją podległą ministrowi właściwemu do spraw informatyzacji i realizować szereg zadań, które dotychczas są przypisane ministrowi, to zakres działania i stopień swobody powinien być uregulowany przez nadzorującego. Ponadto oceniono, że wiele kwestii zostało uszczegółowionych bądź uregulowanych w jaśniejszy sposób, m.in. kwestia zatwierdzenia planu na podstawie kwot ujętych w budżecie itd.

Zwrócono uwagę, że Agencja - przejmując duży zakres działania ministra właściwego do spraw informatyzacji oraz wchodząc w obszary innych instytucji, w tym ministerstw czy różnego rodzaju organów centralnych i przejmując pewne zadania, jak np. nadzorowanie centralnej bazy danych - uzyska unikalne informacje w dwóch obszarach. Po pierwsze, w skali rzeczywistego zinformatyżowania w poszczególnych resortach, branżach, instytucjach itd., a z drugiej strony wiedzę o oczekiwaniach, wiedzę o podmiotach występujących w tym obszarze na rynku oraz oferowane rozwiązania itd. Zaproponowano dopisanie do zadań Agencji w statucie, który nada minister właściwy do spraw informatyzacji, że prezes Agencji corocznie przedstawi raport o stanie informatyzacji w państwie, ze szczególnym wskazaniem rezultatów działań oraz zakresu spraw do wykonania. Taki zapis, oparty o faktyczną wiedzę i realne zdarzenia, stanowiłby materiał do dyskusji z zakresu nowelizacji ustaw czy propozycje do budżetu państwa itd.

Na zakończenie swojego wystąpienia Pan Wiceprzewodniczący wskazał, że konsultacje projektu ustawy o przekształceniu Centralnego Ośrodka Informatyki w Agencję Informatyzacji przyniosły bardzo dobry efekt, a finalna postać dokumentu jest zadowolająca i wychodzi naprzeciw większości zgłaszanych uwag. Projekt ustawy będzie podlegał dalszym modyfikacjom w trybie procedury legislacyjnej zwłaszcza w Sejmie.

Obecny na posiedzeniu Pan Minister Janusz Cieszyński uznał, że cały proces dyskusji był korzystny dla kształtu projektu ustawy.

W dalszej części posiedzenia wspomniano o projekcie nowelizacji ustawy o informatyzacji podmiotów realizujących zadania publiczne, szczególnie w zakresie metod potwierdzania tożsamości i weryfikacji osoby, która chciałaby skorzystać z usług online. Uznano, że jest to kwestia do głębszej analizy przez Radę.

Dyskutowano o terminach kolejnych posiedzeń Rady oraz o tematach, nad którymi Rada będzie obradować. W toku dyskusji Pan Przewodniczący wspomniał, że Pan Wiceprzewodniczący dokonał redakcji protokołów z posiedzeń Rady. Wspomniano także o dokumencie stworzonym w gronie Rady, tj. Rozwój sieci szerokopasmowych i 5G.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Konrad Ciesiołkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Michał Kanownik
6. Janusz Kosiński
7. Karol Krawczyk
8. Dariusz Milka - Wiceprzewodniczący
9. Józef Orzeł – Przewodniczący
10. Bolesław Piasecki
11. Paweł Śniatała
12. Robert Trętowski
13. Mateusz Tykierko

Zaproszeni goście:

14. Janusz Cieszyński, Sekretarz Stanu w KPRM, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
15. Anna Gos, Dyrektor Departamentu Zarządzania Danymi w KPRM
16. Dominik Sybilski, Naczelnik Wydziału w Departamencie Zarządzania Danymi w KPRM
17. Jarosław Mojsiejuk, ekspert Rady
18. Wiesław Paluszyński, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

19. Natalia Matyba, Zastępca Dyrektora Departamentu Polityki Cyfrowej w KPRM
20. Michał Mucha, Zastępca Dyrektora Centrum Rozwoju Kompetencji Cyfrowych w KPRM
21. Anna Biała, Zastępca Dyrektora Departamentu Tożsamości Cyfrowej w KPRM
22. Tomasz Opolski, Zastępca Dyrektora Departamentu Telekomunikacji w KPRM
23. Maciej Górski, Dyrektor Departamentu Zarządzania Systemami w KPRM
24. Joanna Malczewska, Radca w Departamencie Zarządzania Danymi w KPRM

25. Maria Wójtowicz, Starsza kierowniczka projektu, Departament Zarządzania Systemami w KPRM
26. Anna Uzdowska, KPRM
27. Joanna Laskowska, KPRM