RODO-we podchody

Chociaż RODO już nie wzbudza takich emocji jak w latach 2016–2018, nieustannie pojawiają się nowe problemy. Przyjrzyjmy się niektórym z nich.

Joanna Karczewska

absolwentka Wydziału Elektroniki PW z ponad 40-letnim doświadczeniem w informatyce. Jako certyfikowany audytor systemów informatycznych – CISA – specjalizuje się w audytach informatycznych w jednostkach sektora finansów publicznych. Pełni także funkcję inspektora ochrony danych w placówkach oświatowych. Jako Expert Reviewer uczestniczyła w opracowaniu metodyk COBIT5 i COBIT 2019, ITAF 4th Edition oraz publikacji ISACA dotyczących Digital Trust Ecosystem Framework. Bierze udział w konsultacjach aktów prawnych dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych, również na forum Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP. Uznana w 2022 roku za jedną z Europe's Top Cyber Women. Ekspert Najwyższej Izby Kontroli.

We wrześniu 2024 r. w Parlamencie Europejskim przedstawiono raport o przyszłości europejskiej konkurencyjności, w którym zapowiedziano usunięcie wielu barier regulacyjnych, by zachęcić innowacyjne startupy do intensyfikacji działalności w Europie. Założenia przedstawiono w ulotce Komisji Europejskiej https://ec.europa.eu/commission/presscorner/api/files/attachment/880407/Factsheet_Simplification.pdf.

Przepisowe zachcianki

Od lutego 2025 r. zbieraniem propozycji deregulacji w różnych obszarach w Polsce zajął się zespół Rafała Brzoski. Ze zgłoszonymi pomysłami można się zapoznać na specjalnej stronie https://sprawdzamy.com. Nie zdziwiło mnie, że zgłoszono temat obciążeń administracyjnych dla mikro- i małych przedsiębiorców związanych z ochroną danych osobowych. Jak to trafnie ujęto: „Aktualne rozwiązania stanowią istotny koszt dla wyżej powołanych przedsiębiorców, a jednocześnie nie implikują zwiększenia poziomu ochrony danych osobowych. Tym samym aktualne rozwiązania mogą być uznane jako nadmiarowe, a zatem niespełniające wymogu proporcjonalności". Stwierdzono także, że „obowiązki informacyjne są zbyt rozbudowane względem możliwości najmniejszych firm, które często nie mają dostępu do specjalistycznej wiedzy czy zasobów". Zaproponowano uchylenie art. 4a Ustawy o prawach konsumenta, który dotyczy obowiązków informacyjnych wyłącznie w relacji przedsiębiorca–konsument oraz uzupełnienie Prawa przedsiębiorców. Co zaskakujące, osobą promującą te rozwiązania jest Maciej Kawecki (dla niewtajemniczonych – Maciej Kawecki był twarzą RODO, a formalnie – koordynatorem krajowej reformy ochrony danych osobowych w latach 2017–2019, czyli odpowiadał za narzucenie mikro- i małym przedsiębiorcom obowiązku przekazywania szczegółowych informacji dotyczących przetwarzania danych osobowych zgodnie z art. 13 i 14 RODO, takich samych jak w przypadku dużych firm). Jak wynika z komunikatu na stronie https://sprawdzamy.com/pomysl/rodo-dla-malych-firm-mniej-formalnosci-ta-sama-ochrona-id-1645, inicjatywa została przekazana stronie rządowej i na razie jest wstrzymana, bowiem wymaga doprecyzowania i nie jest gotowa do przyjęcia. Trwają wyjaśnienia z zespołem ekspertów i dalsze prace po stronie zespołu SprawdzaMY. Czyżby nici z deregulacji?

Sugeruje to wypowiedź rzecznika UODO, Karola Witowskiego, udzielona podczas wywiadu dla portalu CyberDefence24 (https://cyberdefence24.pl/polityka-i-prawo/rodo-zbyt-surowe-dla-msp-uodo-reaguje-na-propozycje-zespolu-brzoski): „Z obserwacji Prezesa UODO wynika, że małe firmy już się przyzwyczaiły do obowiązków wynikających z RODO. Przez ponad rok spotkań z organizacjami przedsiębiorców nie spotkaliśmy się z wyrażoną potrzebą zmian art. 13 i 14. Warto podkreślić, że zgodnie z proponowanymi zmianami obowiązki z ww. artykułów Rozporządzenia miałyby być przekazywane osobie, której dane dotyczą, na jej żądanie, czyli i tak MSP muszą być przygotowane na spełnienie wobec danej osoby obowiązków informacyjnych wynikających z RODO".

Przepisowe przepychanki

W numerze 1/2025 „Domeny" cieszyłam się z odwołania projektu Centralnej Informacji Emerytalnej (CIE). Pod względem cyberbezpieczeństwa i ochrony naszych danych osobowych oraz prywatności był to koszmarny potworek. Zupełnie nieprzygotowany technicznie i organizacyjnie podmiot miał wiedzieć o nas więcej niż Zakład Ubezpieczeń Społecznych – istny horror! Okazuje się, że 2 kwietnia 2025 r. zespół deregulacyjny Rafała Brzoski zarejestrował pomysł o nazwie mEmerytura, czyli wszystkie dane o Twojej emeryturze w jednym miejscu. Cel jest podobny: udostępnienie obywatelom – raz w roku w aplikacji mObywatel – informacji o ich środkach zgromadzonych w programach emerytalnych ZUS, OFE, PPE, PPK, IKE, IKZE. Jak zaznaczono w zgłoszeniu: „Koszt przeprowadzenia zmian jest niewielki – wymaga wprowadzenia wymogu przekazania jeden raz rocznie informacji o stanach rachunków do jednego podmiotu i połączenia tej informacji z aplikacją mObywatel". Dodam, że wymóg ma dotyczyć wszystkich Polaków. Ponadto „po stronie zarządzającego aplikacją mObywatel będą koszty dostosowania aplikacji i stworzenia modułu mEmerytura". Portal SprawdzaMY nie podał, na czym ma polegać deregulacja, bo raczej jest to zabawa w kotka i myszkę. Nie chcecie PFR-u, to my sobie założymy bazę w mObywatelu.

> *Po co Ministrowi Cyfryzacji wiedza o naszych emeryturach? Dlaczego miałby wyręczać ZUS, który stale i konsekwentnie stoi na straży naszych danych?*

Rozbawił mnie zapis w rubryce „Ocena skutków regulacji". Pomysłodawcy stwierdzili lakonicznie, że jedynym skutkiem będzie „zwiększenie stanu wiedzy obywateli na temat ich oszczędności emerytalnych". To może w następnym kroku również banki będą co roku wysyłać salda naszych rachunków do mObywatela, by zwiększyć stan wiedzy Polaków na temat ich oszczędności złotówkowych? Jak wynika z komunikatu na stronie https://sprawdzamy.com/pomysl/memerytura---wszystkie-dane-o-twojej-emeryturze-w-jednym-miejscu-id-1610, rządowy zespół deregulacyjny we współpracy z Ministerstwem przyjął inicjatywę do wdrożenia. Procedowane są dalsze prace nad przedstawioną dokumentacją w celu przekazania jej do KPRM.

Tymczasem 7 maja 2025 r. pojawił się nowy, konkurencyjny pomysł stworzenia ZUS HUB-u (https://sprawdzamy.com/pomysl/lepszy-dostep-do-danych-emerytalnych-w-jednym-miejscu-dzieki-zus-hub-id-2036/). Te same zadania, inny

wykonawca. W uzasadnieniu podano, że „zgodnie publikowanymi scenariuszami, ok. 70% osób w wieku 40+ i 50+ otrzyma w przyszłości wręcz **głodowe emerytury** – w wysokości minimalnej albo nawet niższej". Korzyścią ma być „możliwość wykorzystania danych do lepszego projektowania polityk publicznych". CIE miała być dobrowolna, eEmerytura lub ZUS-HUB będzie obowiązkowa. Skoro, jak widać, decydenci będą wszystkimi siłami dążyć do utworzenia wspólnej bazy naszych oszczędności emerytalnych, to ZUS faktycznie jawi się jako „naturalny kandydat na centralnego operatora takiej platformy", bowiem faktycznie „posiada już infrastrukturę i zaufanie społeczne" oraz najwięcej danych o naszych emeryturach.

Przepisowi strażnicy

Strażnikami prawa są prawnicy. Powinni być dla nas wzorem przestrzegania wszelkich ustaw, rozporządzeń i regulaminów. Życie pisze jednak swoje scenariusze. Najlepszym przykładem jest casus Naczelnej Rady Adwokackiej (NRA), która od kilku lat implementuje i eksploatuje elektroniczny system obsługi Adwokatury, zwany e-SOA, przetwarzający m.in. dane osobowe adwokatów. W związku z jego wdrożeniem w 2023 r. NRA opublikowała poradnik „Dobre praktyki cyberbezpieczeństwa w pracy adwokata i kancelarii", o którym pisałam w nr 2/2023 „Domeny". W przypadku korzystania z aplikacji lub usług zewnętrznego wsparcia informatycznego, w ramach których dostawcy uzyskują dostęp do danych osobowych przetwarzanych przez kancelarię adwokacką, zalecano zachowanie zasad bezpieczeństwa i poufności danych zgodnie z normami z serii ISO/IEC 27000 oraz zawarcie stosownej umowy powierzenia przetwarzania danych osobowych zgodnej z przepisami RODO i zasadami dostępu do Tajemnicy zawodowej. W 2018 r. NRA opublikowała także Przewodnik po RODO dla adwokatów, w którym znalazły się informacje, jak zawrzeć umowę powierzenia i co powinna zawierać. Zatem NRA miała własne źródła wiedzy o ochronie danych i cyberbezpieczeństwie.

W swoim artykule przed rokiem zainteresowałam się, jak przebiega wdrożenie systemu zarządzania bezpieczeństwem informacji w NRA. Jak wygląda jego stałe i konsekwentne stosowanie brutalnie przekonało się kilka tysięcy adwokatów i aplikantów adwokackich, których dane 27 grudnia 2024 r. zostały ujawnione przez cyberprzestępców w internecie (https://cyberdefence24.pl/polityka-i-prawo/wyciek-danych-tysiecy-adwokatow-zrodlem-nie-bylo-nra). Informacja o naruszeniu ochrony danych dotarła do zainteresowanych dopiero 14 lutego 2025 r., ale resetu haseł dostępu do Panelu Adwokata e-SOA zespół ds. wdrożenia i rozwoju systemu dokonał już 9 stycznia 2025 r. NRA tak się tłumaczyła dziennikarzowi CyberDefence24: „Wstępne ustalenia wskazują, że ewentualny wyciek nie pochodził z infrastruktury Naczelnej Rady Adwokackiej, lecz mógł pochodzić z infrastruktury podmiotu współpracującego z NRA przy budowie systemu informatycznego, który posiadał dane na podstawie prawidłowego ich powierzenia". Czyli klasyka: to nie nasza wina, to oni.

Warto przypomnieć, że w podobnym przypadku kierownik basenu w Kutnie dostał od Prezesa UODO wysoką karę za „naruszenie przepisu art. 28 ust. 1 RODO, polegające na braku weryfikacji podmiotu przetwarzającego, pod kątem ustalenia, czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą".

13 lutego 2025 r. NRA zaprosiła do składania ofert na świadczenie stałej obsługi informatycznej w zakresie administracji i zapewnienia bezpieczeństwa swoich serwerów chmury, stron internetowych, oprogramowania dedykowanego oraz zasobów lokalnych. Zakres oferty obejmował „współpracę z inspektorem ochrony danych osobowych Zleceniodawcy dotyczącą bezpieczeństwa informacji w zakresie doradztwa w przedmiocie analizy bezpieczeństwa IT, procesów biznesowych w ramach infrastruktury Zleceniodawcy oraz rekomendacji w zakresie bezpieczeństwa IT zgodnie z dobrymi praktykami". Czyżby wcześniej NRA nie miała fachowego wsparcia informatycznego? Na decyzję prezesa UODO w sprawie wycieku przyjdzie nam poczekać co najmniej 2 lata.

Na razie prezes UODO zwrócił uwagę, że przepisy art. 58a Prawa o adwokaturze, jak i rozporządzenia z 2016 roku w sprawie minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania systemu teleinformatycznego, w którym NRA prowadzi listę adwokatów, aplikantów adwokackich oraz prawników zagranicznych, nie zawierają wystarczających rozwiązań prawnych zapewniających stosowanie przepisów RODO w odniesieniu do przetwarzania danych osobowych w e-SOA. Zrobił to w styczniu 2025 r. przy okazji konsultowania wniosku NRA o dofinansowanie budowy i wdrożenia e-SOA 2.0 z Funduszy Europejskich na Rozwój Cyfrowy 2021–2027 (https://www.gov.pl/web/cppc/nadchodzi-esoa-2.0).

Prawnicy ciągle nas pouczają, a sami nie potrafią sprostać własnym przepisom.

Przepisowi pomocnicy

Ostatnio prawnicy wywołali burzę w szklance wody wokół nowej, drugiej wersji poradnika UODO dotyczącego

obowiązków administratorów związanych z naruszeniami ochrony danych osobowych. Jedni uznali, że prezes UODO zaciemnił obraz tego, czym ma zajmować się inspektor ochrony danych (IOD) w ramach obsługi naruszeń. Inni zgodzili się z tezami prezesa. Przy okazji dowiedzieliśmy się, co jeden ze znanych radców prawnych rekomenduje swoim klientom. Otóż od lat powtarza na szkoleniach dla zarządów, żeby administratorzy, poza IOD, powoływali także SOD, czyli specjalistę od ochrony danych – administrator może powierzyć odpowiedzialność za ochronę danych dowolnej osobie, byle nie był nią IOD. Czyżby szykowało się kolejne obciążenie dla mikro-, małych i średnich przedsiębiorców?

Spory prawników dotyczą stopnia niezależności IOD. Prezes UODO tak ich definiuje w przywołanym poradniku: „Inspektorzy ochrony danych to profesjonalni doradcy wspierający administratorów i podmioty przetwarzające w zapewnieniu zgodności z przepisami RODO. Aby prawidłowo wykonywać swoje zadania, IOD muszą być niezależni, a zakres ich odpowiedzialności powinien być wolny od konfliktu interesów". W grudniu 2024 r. nałożył wysoką karę na Toyota Bank Polska SA za niezapewnienie przez bank (jako administratora), by inspektor ochrony danych podlegał bezpośrednio najwyższemu kierownictwu i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Prezes uznał, że zatrudnienie IOD na stanowisku IT audytora/specjalisty ds. bezpieczeństwa w zespole ds. bezpieczeństwa w departamencie bezpieczeństwa i jego bezpośrednia podległość dyrektorowi tego departamentu nie zapewnia niezależności IOD i narusza art. 38 ust. 3 RODO. Ministerstwo Finansów w swoim regulaminie organizacyjnym załatwiło to tak: w zakresie realizacji zadań, o których mowa w art. 39 RODO, i innych przepisów dotyczących ochrony danych osobowych IOD podlega bezpośrednio Administratorowi tych danych, zaś Departament Bezpieczeństwa odpowiada za obsługę organizacyjną IOD.

> *Od początku intryguje mnie zapis art. 38 ust. 3 RODO, że IOD nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Czy regulatorom naprawdę zależało na stworzeniu kasty nietykalnych pomocników, którzy za nic nie odpowiadają i których administratorzy danych nie mogą rozliczać?*

W naszej ustawie o ochronie danych osobowych do wyznaczenia niezależnych IOD zobowiązano wszystkie jednostki sektora finansów publicznych. W samej Warszawie jest to urząd miasta i 1268 jednostek podległych. Jednostki samorządowe przetwarzają mnóstwo danych osobowych, zatem każda pomoc się przyda.

W kwietniu 2025 r. Najwyższa Izba Kontroli opublikowała raport z kontroli zapewnienia bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w 24 jednostkach samorządu terytorialnego (https://www.nik.gov.pl/aktualnosci/cyberbezpieczenstwo-w-samorzadach-2025.html). Badanie zostało przeprowadzone w 2024 r. i dotyczyło okresu od 1.01.2023 r. do 20.09.2024 r. Jego wyniki jednoznacznie wskazują, że pomoc ze strony IOD-ów jest słaba. Owszem, NIK potwierdziła niezależność IOD-ów we wszystkich badanych jednostkach oraz ich kompetencje. Jednak nasuwa się pytanie, jaka jest ich przydatność, skoro tylko jedna jednostka otrzymała pozytywną ocenę ogólną za realizację działań z kontrolowanego obszaru, zaś aż dwie otrzymały ocenę negatywną (Starostwa Powiatowe w Ostrołęce i w Sochaczewie). W 8 jednostkach nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, a w 3 jednostkach, gdzie SZBI został ustanowiony, nie dokonano jego przeglądu pod względem adekwatności i skuteczności.

Najbardziej martwi, że 71% skontrolowanych urzędów nie było przygotowanych do zapewnienia ciągłości działania systemów informatycznych. W 12 urzędach (połowa) stwierdzono nieprawidłowości polegające na niewłaściwym przechowywaniu kopii zapasowych, niesporządzaniu kopii zapasowych lub tworzeniu ich niezgodnie z przyjętymi procedurami oraz braku testowania kopii zapasowych. Dostępność i odporność systemów i usług przetwarzania są podstawowym wymogiem stawianym administratorom danych, zaś §19 ust. 2 Rozporządzenia o KRI zawiera listę podstawowych działań, które należy wykonywać, by wypełniać obowiązki wynikające z art. 32 RODO. Dlaczego IOD-y nie zwrócili na to uwagi?

Przyjrzałam się też ustaleniom dotyczącym szkoleń. Aż w 10 jednostkach ich nie organizowano. W Starostwie w Sochaczewie IOD prowadził szkolenia zapoznające pracowników urzędu z przepisami RODO oraz dokumentacją opisującą zasady przetwarzania danych w urzędzie; nikt nie prowadził szkoleń z zakresu bezpieczeństwa informacji. Z kolei w Starostwie w Ostrołęce zorganizowano szkolenia z ochrony danych osobowych tylko w 2023 r.; nie zapewniono szkoleń z zakresu bezpieczeństwa informacji. Pytanie do IOD-ów: jak uczycie bezpiecznego przetwarzania danych osobowych, skoro nie uczycie bezpiecznego przetwarzania informacji?

Przepisowa inteligencja

Może pomoże sztuczna inteligencja? 7 maja 2025 r., na posiedzeniu Komisji Cyfryzacji Sejmu RP, Dariusz Standerski, sekretarz stanu w Ministerstwie Cyfryzacji, przedstawił informację o szkoleniach z zakresu sztucznej inteligencji dla administracji publicznej prowadzonych przez Ministerstwo Cyfryzacji. Okazuje się, że w IV kwartale 2024 r. przeszkolonych zostało 2400 pracowników różnych ministerstw, w tym 200 osób z Ministerstwa Finansów. Celem było podniesienie kompetencji urzędników, by bezpiecznie i odpowiedzialnie korzystali z AI w sektorze publicznym. Szczególną uwagę poświęcono kwestiom etycznym, ochronie danych osobowych oraz zgodności z obowiązującymi przepisami. Resortom zostanie udostępniony polski PLLuM. Podobno urzędnicy nie będą wykorzystywać sztucznej inteligencji do pisania uzasadnień decyzji administracyjnych. Pożyjemy, zobaczymy.

Zainteresowały mnie plany Ministerstwa Finansów dotyczące stosowania sztucznej inteligencji. Już w 2021 r. przyjęto „Strategię Robotyzacji w Ministerstwie Finansów", która zakłada, że „wszystkie działania związane z analizą, wytwarzaniem, testowaniem i utrzymaniem robotów powinny być prowadzone zgodnie z zasadami określonymi w Polityce Ochrony Danych Osobowych oraz zgodnie z polityką bezpieczeństwa informacji". W 2022 r. powołany został Pełnomocnik Ministra Finansów do spraw Rozwoju Sztucznej Inteligencji, którego zadaniem jest m.in. koordynowanie wdrożenia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" przyjętej przez Radę Ministrów w 2020 r., przypominającej o poszanowaniu prywatności i zasad ochrony danych osobowych. Według aktualnego regulaminu organizacyjnego sztuczną inteligencją zajmują się:

- Departament Transformacji Cyfrowej w zakresie koordynowania i opiniowania rozwiązań teleinformatycznych wykorzystujących metody AI,
- Departament Strategii w zakresie rozwoju produktów analityki danych z wykorzystaniem metod AI (raporty i analizy strategiczne),
- Departament Analiz Krajowej Administracji Skarbowej (KAS) w zakresie tworzenia produktów zaawansowanej analityki danych w oparciu o metody AI.

Ostatnio dwie posłanki Sejmu RP, niezależnie od siebie, spytały Ministerstwo Finansów o korzystanie z AI. Z odpowiedzi na interpelację nr 9137 dowiadujemy się, że KAS wykorzystuje uczenie maszynowe w procesach analitycznych, które wspomaga jej jednostki w działaniach analitycznych dotyczących identyfikacji i zwalczania nadużyć podatkowych, a Ministerstwo prowadzi prace pilotażowe, mające na celu potwierdzenie możliwości zastosowania rozwiązań wykorzystujących nowe technologie: RPA, ML czy AI w narzędziach wspierających pracę zespołów back office. Z kolei na pytanie: „Jakie mechanizmy bezpieczeństwa zostały wprowadzone w związku z wykorzystywaniem technologii AI w celu ochrony wrażliwych danych podatkowych i osobowych?" zadane w interpelacji nr 8393 Ministerstwo odpowiedziało, że jest wdrożony i doskonalany System Zarządzania Bezpieczeństwem Informacji, zgodnie z Rozporządzeniem o KRI i zgodnie z normą ISO/IEC 27001. ŁAŁ!

Przepisowe wykluczenie

W numerze 1/2025 „Domeny" wspomniałam o mojej sprawie. Zainteresowanych pragnę poinformować, że prezes UODO wydał obie zapowiadane decyzje, a ja obydwie zaskarżyłam do Wojewódzkiego Sądu Administracyjnego w Warszawie. Znów poczekam kilka miesięcy na kolejne rozstrzygnięcie. Najbardziej pesymistyczna wizja finału mojej historii przedstawia się następująco:

Zgodnie z panującym trendem Ministerstwo Finansów/Krajowa Administracja Skarbowa wdrażają PLLuM-a w ciągu najbliższych miesięcy. Urzędnicy trenują model językowy na przepisach FATCA (Foreign Account Tax Compliance Act) z pominięciem amerykańskich przepisów dotyczących obywatelstwa, na danych przekazanych automatycznie z systemu KAS do USA oraz na moich sprawach z ING Bank Śląski SA i – identycznej – z BNP Paribas Bank Polska S.A. PLLuM dochodzi do wniosku, że wszystkie banki w Polsce powinny mnie oraz 1294 (tysiąc dwustu dziewięćdziesię-ciu czterech) pozostałych obywateli polskich urodzonych w Stanach Zjednoczonych i niepodlegających *jus soli* (z łac. prawo ziemi) potraktować równo, czyli wypowiedzieć im umowy na świadczenie usług. Przygotuje stosowny dokument, który urzędnicy ministerialni skrzętnie podpiszą i wyślą do wszystkich banków działających w Polsce. Banki dadzą nam miesiąc na spłatę wszelkich należności i wypłacenie gotówki, zanim zablokują nam dostęp do naszych rachunków. Staniemy się **Polakami wykluczonymi bankowo** przez własną ojczyznę. Wszystko w majestacie prawa z błogosławieństwem Ministra Finansów. O innych konsekwencjach prywatnych i zawodowych nawet nie wspomnę. Żadna instytucja krajowa nam nie pomoże. Jest nas za mało, by politycy się nami przejęli. Będziemy pierwszymi ofiarami poważnego incydentu w rozumieniu art. 3 pkt 49 unijnego Aktu w sprawie sztucznej inteligencji, wręcz męczennika-mi z powodu mody na bezmózgowe myślenie maszynowe, przy totalnym ignorowaniu Rezolucji P8_TA(2018)0316 Parlamentu Europejskiego z dnia 5 lipca 2018 r. o szkodliwych skutkach FATCA dla obywateli UE.

Znając polskie realia, tak właśnie będzie.

P.S. Właśnie mBank idzie w ślady ING.

Informacje w artykule są podane według stanu na 15 maja br.