Cyber-odklejka

Słowo „odklejka" otrzymało Nagrodę Jury w plebiscycie Młodzieżowe Słowo Roku 2022 zorganizowanym przez Wydawnictwo Naukowe PWN. Odklejka oznacza stan, ewentualnie osoby, które są oderwane od rzeczywistości i dotyczy zarówno zachowania, jak i wypowiadanych treści. W przypadku cyberbezpieczeństwa i ochrony danych osobowych oznacza oderwanie przyjętych deklaracji i działań od rzeczywistych potrzeb i faktów. Oto kilka przykładów z bardzo różnych obszarów.

Joanna Karczewska
audytor SI, ekspert ds. cyberbezpieczeństwa
i ochrony danych osobowych

Od ponad dwudziestu lat jestem klientką ING Banku Śląskiego. Mam w nim zarówno konto osobiste, jak i firmowe. Wydawało się, że obie strony są zadowolone. Do czasu. W połowie kwietnia ub.r. bank poinformował, że zidentyfikował mnie jako rezydenta podatkowego USA, bo urodziłam się w USA. W związku z FATCA bank przekaże moje dane do Internal Revenue Service USA za pośrednictwem Krajowej Administracji Skarbowej.

Cel FATCA

Celem automatycznej wymiany informacji o amerykańskich rachunkach raportowanych (FATCA) jest umożliwienie administracji podatkowej pozyskiwania z instytucji finansowych określonych z góry informacji o amerykańskich rachunkach raportowanych, **zidentyfikowanych** jako prowadzone dla amerykańskich osób raportowanych, w ustalonych z góry, regularnych odstępach czasu. Uzyskane w tym trybie informacje będą w dalszej kolejności podlegały systematycznemu przekazywaniu Stanom Zjednoczonym Ameryki.

https://www.podatki.gov.pl/podatkowa-wspolpraca-miedzynarodowa/automatyczna-wymiana-informacji-podatkowych/fatca/

Bank zamierzał całkowicie zablokować mi dostęp do rachunków – na dwa dni przed terminem rozliczeń z ZUS-em i organem podatkowym. Po awanturze w oddziale bank w swojej łaskawości pozostawił mi dostęp, ograniczony do funkcji wykonywania przelewów i pobierania wyciągów, zaś przy każdym logowaniu do bankowości elektronicznej pojawia się następujący komunikat:

Wyślij brakujący skan lub zdjęcie dokumentu

Aby Twoje oświadczenie o rezydencji podatkowej FATCA było ważne, wyślij nam skan lub zdjęcie jednego z poniższych:

- zaświadczenie o utracie obywatelstwa USA
- wyjaśnienie, dlaczego nie uzyskałeś amerykańskiego obywatelstwa z chwilą narodzin
- zaświadczenie o zrzeczeniu się statusu stałego rezydenta USA.

Potrzebujemy tego, aby potwierdzić, że nie jesteś rezydentem podatkowym Stanów Zjednoczonych Ameryki. Dopóki tego nie potwierdzimy, nie możesz skorzystać z naszej oferty.

W świetle prawa polskiego i prawa amerykańskiego jestem tylko i wyłącznie obywatelką Rzeczpospolitej Polskiej. Zatem przekazanie moich danych do IRS USA jest **bezprawne i nielegalne**, a żądanie ode mnie wymienionych dokumentów – żenujące, bo świadczy o kiepskim przygotowaniu banku do FATCA. Automatyzacja nie zawsze dobrze się kończy.

Rozpoczęłam działania zmierzające do wstrzymania przekazania.

1. Rozmawiałam z dyrektorem oddziału banku – rozłożył ręce, słałam wiadomości przez system – bez odzewu, skontaktowałam się z Inspektorem ochrony danych banku w Polsce – udzielał standardowych odpowiedzi, na dodatek z błędami i niekompletnych, oraz napisałam do Chief Compliance Officer, ING Group, Amsterdam, Netherlands – bez odzewu.
2. Napisałam do Krajowej Administracji Skarbowej – bez odzewu.
3. Sprawdziłam zakresy obowiązków komórek organizacyjnych Ministerstwa Finansów w sprawie FATCA i napisałam do:
   - Departamentu Podatków Dochodowych – odpowiedział Departament Polityki Podatkowej odsyłając do banku,
   - Departamentu Polityki Podatkowej – ponownie odesłał do banku,
   - Inspektora ochrony danych – zdawkową odpowiedź otrzymałam od wicedyrektora Departamentu Bezpieczeństwa i Ochrony Informacji.

Wszyscy mnie zbywali, zaś dane zostały automatycznie przekazane. Teraz czekam na ciąg dalszy. Może uzbrojeni funkcjonariusze KAS odwiedzą mnie o szóstej rano? A może strona amerykańska wykaże stronie polskiej, że popełniła błąd?

Przeraziła mnie odklejka zainteresowanych podmiotów:

- **brak dociekania i działania w sprawie poważnego incydentu, czyli bezprawnego i nielegalnego przekazania danych do państwa trzeciego, szczególnie ze strony IOD banku oraz IOD i DB MF,**
- **brak znajomości przepisów polskich i amerykańskich,**
- **brak poszanowania mojej prywatności oraz**
- **brak ochrony obywateli RP ze strony organów państwa.**

Z powodu FATCA podobne przykrości spotkały moją rodzinę w BNP Paribas. Na razie nie zgłosiłam do UODO naruszenia ochrony moich danych osobowych i nie złożyłam pozwu do sądu w Katowicach. Zależało mi na zapobieżeniu przekazania, a nie na kilkuletnich postępowaniach administracyjnych czy procesowych, które wiązałyby się m.in. z opowiadaniem mojego życiorysu ze szczegółami zupełnie obcym ludziom, czyli naruszeniem mojej prywatności.

Zadziwiające orzecznictwo

Skoro wspomniałam o sądach, to ostatnio zaintrygowało mnie orzecznictwo Wojewódzkiego Sądu Administracyjnego w Warszawie w sprawach dotyczących ochrony danych osobowych. Dotychczas w swoich postępowaniach WSA bazował na kilku komentarzach, pisanych naprędce po przyjęciu RODO w 2016 r. przez rywalizujące grupy prawników – naukowców i teoretyków, którzy nigdy nie zajmowali się ochroną danych osobowych praktycznie i na co dzień. Stąd m.in. wpadka z pojęciem „*documented instructions*" z artykułu 28 Podmiot przetwarzający. Jego błędna interpretacja jako „udokumentowanego polecenia" do dziś dnia stwarza poważne problemy w umowach z dostawcami usług informatycznych. Nikt nie ma jednak odwagi ogłosić sprostowania oraz przeprosić za zamieszanie i powstałe absurdy.

Teraz sędziowie mają zagwozdkę, bowiem coraz częściej w sprawach RODO istotne są kwestie techniczne, wynikające przede wszystkim z zapisów artykułu 32 Bezpieczeństwo przetwarzania, zaś możliwe do zastosowania środki techniczne i organizacyjne są ujęte nie w samych przepisach czy komentarzach prawnych, a w międzynarodowych i polskich standardach, normach i dobrych praktykach dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa, które trzeba znać i rozumieć.

Ilustracją problemu jest sprawa kary administracyjnej nałożonej na Virgin Mobile [sygnatura akt II SA/Wa 272/21] za naruszenie art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1, art. 32 ust. 1 lit. b i lit. d oraz art. 32 ust. 2 RODO poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych. Sąd uchylił zaskarżoną decyzję. Jednocześnie potwierdził ocenę Prezesa UODO przyjętych środków technicznych i organizacyjnych bez własnej weryfikacji:

- **Zdaniem Sądu** w kontekście ww. przepisów **prawidłowe było stanowisko organu**, że przyjęty przez Spółkę środek bezpieczeństwa, mający zapewnić odporność systemów informatycznych, …
- **Rację miał również Prezes UODO**, wskazując w uzasadnieniu zaskarżonej decyzji, że brak w przyjętych przez Spółkę procedurach uregulowań zapewniających regularne testowanie, mierzenie i ocenianie skuteczności …
- **W ocenie Sądu** w okolicznościach faktycznych sprawy **zastrzeżeń nie budzi także stanowisko Prezesa UODO**, że do wykrycia wykorzystanej podatności systemu, która doprowadziła do naruszenia ochrony danych osobowych, wystarczyłoby zweryfikowanie podstawowej zasady działania systemu …
- **Sąd zgadza się ze stanowiskiem Prezesa UODO** wyrażonym na s. 14 zaskarżonej decyzji, odnoszącym się do konkretnych argumentów podnoszonych w postępowaniu przez Spółkę, że dokonywanie testów …
- **Zdaniem Sądu rację miał więc organ**, że przyjęta przez Spółkę ocena ryzyka …

Na dodatek Sąd ujawnił informacje, które Prezes UODO skrzętnie ukrył w swojej decyzji. W akapicie zaczynającym się od „**Za trafne, spójne, logiczne i wynikające ze stanu faktycznego należało także uznać oceny Prezesa UODO**, że przyjęte przez Spółkę środki ochrony danych osobowych… w postaci procedur ... i sąd wymienił tytuły wszystkich procedur, polityk i planów zastąpione kwadratowymi nawiasami w decyzji.

MS Teams na straży

Jeszcze bardziej zaskoczyło mnie uzasadnienie wyroku z dnia 19 kwietnia 2022 r. w sprawie o sygnaturze akt II SA/Wa 2259/21. Rozpatrywana była skarga na decyzję Prezesa UODO wniesiona przez S.Z. na nieprawidłowości w procesie przetwarzania danych osobowych jego małoletniej córki Z.Z. przez Szkołę Podstawową nr [...] im. [...] w J. polegające na przetwarzaniu danych osobowych małoletniej Z.Z. za pośrednictwem platformy MS Teams podczas prowadzenia zdalnego nauczania bez podstawy prawnej – zgody rodziców, a w konsekwencji udostępnienia jej danych podmiotowi nieuprawnionemu – operatorowi platformy MS Teams oraz przetwarzaniu jej danych osobowych za pośrednictwem powyższej platformy bez spełnienia obowiązków informacyjnych wynikających z art. 13 i art. 14 RODO.

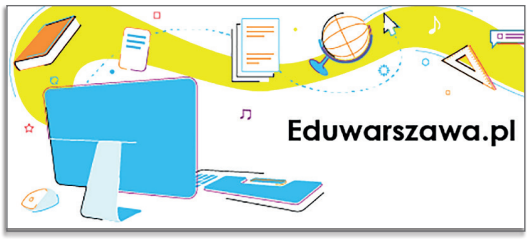
Sąd w składzie 3-osobowym oddalił skargę S.Z. m.in. dlatego, że „wybór przez Szkołę platformy MS Teams prowadzonej przez **profesjonalny podmiot**, jakim jest **renomowana** Microsoft Corporation, która stanowić będzie w tym przypadku procesora (czyli podmiot, który – w ramach powierzenia przetwarzania danych – przetwarza w imieniu administratora dane przez niego powierzone) **z całą pewnością gwarantuje** stosowanie przez podmiot przetwarzający środków organizacyjnych i technicznych, o których mowa w art. 28 ust. 1 RODO".

Chciałoby się rzec: serio? poważnie? Wystarczy, że wdrożymy MS Teams i cyberbezpieczeństwo mamy z głowy?

Podobno z wyrokami sądów się nie dyskutuje. Co jednak oznacza podejście do kwestii technicznych przyjęte przez sędziów WSA? Otóż na zapisy przytoczonych orzeczeń będą powoływać się sędziowie w kolejnych sprawach. Będą powielać oceny poprzedników i rozstrzygać o cyberbezpieczeństwie zamiast nas, fachowców. Ciekawe, kto zajmuje się cyberbezpieczeństwem w samym WSA w Warszawie.

Koszty audytu w oświacie

Nie tylko miejscowość J. zdecydowała się zastosować MS Teams do zdalnego nauczania. Również inne miasta, w tym Lublin, Warszawa i Wrocław, wybrały pakiet Microsoft Office 365 do wdrożenia i rozwoju platform edukacyjnych w szkołach i placówkach, dla których są organem prowadzącym. W przypadku Warszawy jest to jedno z największych edukacyjnych wdrożeń Office 365 Education w Europie (https://news.microsoft.com/pl-pl/features/od-zdalnej-nauki-do-szkoly-przyszlosci-microsoftmowi/).



Jednak najczęściej spotykane w placówkach oświatowych, wręcz wszechobecne, są programy do zarządzania szkół i przedszkoli oferowane przez polską firmę VULCAN Sp. z o.o. z Wrocławia, przy czym są to aplikacje desktopowe bądź hostowane na serwerach firmy.

Każde wdrożenie programu hostowanego poprzedza podpisanie standardowej umowy przetwarzania danych (https://www.vulcan.edu.pl/vulcang_files/user/AABW/AABW-PDF/_do-pobrania/Serwis_UPO-RODO.pdf), zawierającej dość zaskakujące zapisy:

- dotyczące wyłączenia odpowiedzialności: „Przetwarzający [VULCAN] nie ponosi odpowiedzialności za skutki nieprzestrzegania przez Administratora danych [placówka oświatowa] lub osoby działające w jego imieniu zasad bezpieczeństwa przy użytkowaniu systemu. Podstawowe i uniwersalne zasady bezpieczeństwa, do przestrzegania których Administrator danych i osoby działające w jego imieniu są zobowiązani, wskazano pod adresem https://vulcan.edu.pl/strona/bezpieczenstwo-systemow." Po pierwsze RODO nie dopuszcza wyłączenia odpowiedzialności podmiotu przetwarzającego w ramach umowy lub innego instrumentu prawnego. Po drugie zapoznałam się z proponowanymi zasadami bezpieczeństwa i doznałam szoku. Dawno już nie widziałam podobnego miszmaszu. Próbowałam uzyskać informacje, na podstawie jakich powszechnie uznanych standardów, norm i dobrych praktyk opracowano proponowane zasady. Nie udało się.

- dotyczące kontroli: „Obsługa przez Przetwarzającego prowadzonych u niego kontroli procesu przetwarzania danych w formie udzielania na żądanie Administratora danych informacji i wyjaśnień oraz kontroli bezpośrednich również podczas organizowanych przez Przetwarzającego dni otwartych prowadzona jest w ramach **wynagrodzenia** Przetwarzającego".

Tak, tak, jeżeli Administrator danych chce przeprowadzić audyt czy inspekcję na podstawie art. 28 ust. 3 lit. h RODO, to musi zwrócić Przetwarzającemu, czyli firmie VULCAN, koszty obsługi kontroli (https://www.vulcan.edu.pl/strona/koszty-obslugi-kontroli-630). **Horrendalnie** wysoka dla placówek oświatowych opłata ryczałtowa za każdy dzień obsługi kontroli w siedzibie firmy we Wrocławiu (1000 zł netto) i ewentualnie w centrum danych w Katowicach (2000 zł netto), może sprawić, że żadna placówka oświatowa nie zdecyduje się na audyt. Ciekawa jestem, jakie będzie podejście UODO do tej kwestii w przypadku wystąpienia naruszenia. Za brak przestrzegania RODO Prezes UODO może nałożyć na jednostki samorządu terytorialnego kary pieniężne w wysokości do 100 tys. złotych. Jeżeli dojdzie do naruszenia i nałożenia kary w wysokości np. 1000 zł na każdego administratora, czyli każdą placówkę oświatową, to zamiast max. 100 tys. zł miasto Lublin zapłaci prawie 300 tys. zł (wykaz placówek publicznych na stronie EduLublin zawiera 289 pozycji). Ostatnio w ramach centralizacji to władze miast i wsi decydują o wdrożeniu w podległych placówkach konkretnych systemów informatycznych od konkretnych dostawców. Dyrektorzy placówek tylko je realizują. Trudno ich nazwać administratorami danych, skoro nie ustalają ani celów i sposobów przetwarzania danych osobowych w tych systemach, ani środków technicznych i organizacyjnych. Ale karę dostanie każdy z nich.

Za brak przestrzegania RODO Prezes UODO może nałożyć na jednostki samorządu terytorialnego kary pieniężne w wysokości do 100 tys. złotych. Jeżeli dojdzie do naruszenia i nałożenia kary w wysokości np. 1 000 zł na każdego administratora, czyli każdą placówkę oświatową, to zamiast max. 100 tys. zł miasto Lublin zapłaci prawie 300 tys. zł (wykaz placówek publicznych na stronie EduLublin zawiera 289 pozycji). Ostatnio w ramach centralizacji to władze miast i wsi decydują o wdrożeniu w podległych placówkach konkretnych systemów informatycznych od konkretnych dostawców. Dyrektorzy placówek tylko je realizują. Trudno ich nazwać administratorami danych, skoro nie ustalają ani celów i sposobów przetwarzania danych osobowych w tych systemach ani środków technicznych i organizacyjnych. Ale karę dostanie każdy z nich.

Moją współpracę z „Domeną" rozpoczęłam od artykułu o cyber-odklejkach w systemie polskiej oświaty i w kolejnych publikacjach wracałam do tego tematu. To praw-

dziwa neverending story, bo lista absurdów ciągle się wydłuża, a żadna instytucja nie poczuwa się do odpowiedzialności, by podjąć działania naprawcze.

Klucz do zdrowia

Miszmasz znalazłam także w „Kodeksie postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych", opracowanym przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie i zatwierdzonym przez Prezesa UODO w dniu 14 grudnia 2022 r. Funkcję podmiotu monitorującego stosowanie kodeksu będzie pełnić firma RS Jamano.

Kodeks liczy 109 stron i jest zwyczajnym, na dodatek kiepskim, poradnikiem. Przede wszystkim nie zawiera listy standardów, norm i dobrych praktyk dotyczących bezpieczeństwa informacji, z których korzystano przy jego opracowaniu. Podmiot monitorujący – zarazem współautor kodeksu – zaznaczył w nim, że ma zespół ekspertów, którzy w okresie trzech lat poprzedzających zatwierdzenie kodeksu przeprowadzili łącznie co najmniej 500 audytów ochrony danych w podmiotach leczniczych. Zatem, zgodnie z obowiązującymi standardami audytu, do oceny środków technicznych i organizacyjnych zastosowanych dla bezpieczeństwa przetwarzania, musiał stosować kryteria, które były obiektywne, kompletne, relewantne, wymierne, jasne, powszechnie uznane, miarodajne i zrozumiałe lub dostępne dla wszystkich czytelników i użytkowników raportu. Ich lista została jednak pominięta, chociaż nadal będą potrzebne do oceny, skoro opis środków technicznych i organizacyjnych (mechanizmów kontrolnych), które mały podmiot medyczny (MPM) powinien wdrożyć, zawarto na 1 (słownie: jednej) stronie (plus przykład, też na jednej stronie).

Według Cambridge Dictionary „*code of conduct*" to „*set of rules that members of an organisation or people with a particular job or position* ***must*** *follow*". Zwracam uwagę na słowo „must", po polsku „musi". Słowo „musi" pojawia się w kodeksie 60 razy. Za to słowo „należy" występuje 102 razy, zaś słowo „powinien" z odmianami – 94 razy. Zatem w kodeksie mamy do czynienia z tzw. „wishful thinking" (myśleniem życzeniowym), a nie z jednoznacznymi wymaganiami. Mamy także kompletny miszmasz pojęć informatycznych:

- polityki ochrony danych v. polityki bezpieczeństwa,
- audyt ochrony danych v. audyt bezpieczeństwa,
- bazy danych v. moduły w aplikacjach, programach, systemach informatycznych,
- mechanizmy kontrolne, czyli środki techniczne i organizacyjne, o których mowa w RODO, v. środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych z art. 35 RODO.

i brak ich objaśnień, a najważniejsza jest polityka kluczy. Na stronach od 32 do 43 klucze (do szaf czy pomieszczeń) i kluczniki (szafki do przechowywania kluczy) są wymienione trzynaście razy.

Pozostaje pytanie, jak lekarze z MPM zrozumieją słowo klucz pojawiające się w tabeli 10 na stronie 64 w kontekście naruszeń ochrony danych:

- **Zdarzenie: Administrator przechowywał kopię zapasową archiwum danych osobowych, zaszyfrowaną na płycie CD. Płytę skradziono podczas włamania.**
- **Czy należy zawiadamiać Prezesa UODO? Nie.**
- **Czy należy zawiadamiać osobę, której dotyczą dane? Nie.**
- **Uwagi: Jeżeli dane są zaszyfrowane za pomocą algorytmu zgodnego ze stanem techniki, istnieją kopie zapasowe danych, a unikalny klucz jest bezpieczny, może to być naruszenie niepodlegające obowiązkowi zgłoszenia.**

Jest to jedyne użycie słowa klucz w znaczeniu – jak mniemam – klucza do szyfrowania danych i nie ma żadnego wyjaśnienia jego znaczenia. A może chodzi o unikalny klucz do pomieszczenia, gdzie są składowane pozostałe kopie zapasowe danych? Swoją drogą warto zapoznać się z całą tabelą nr 10 zawierającą sugerowane postępowanie MPM w przypadku stwierdzenia określonych rodzajów naruszeń ochrony danych. Skoro została zatwierdzona przez UODO, to stanowi de facto obowiązującą wykładnię postępowania także w innych podmiotach.

W ramach ładu organizacyjnego i kontroli wewnętrznej COSO przyjęty został model trzech linii obrony określający, w jaki sposób konkretne zadania związane z ryzykiem i kontrolą mogą być przypisane i koordynowane w ramach organizacji, niezależnie od jej wielkości i złożoności. Dotyczy to również obrony cyberbezpieczeństwa. Ustanowione są także różne zewnętrzne linie obrony. W opisanych przeze mnie przypadkach wszystkie linie zawiodły. Przyjęte deklaracje i działania okazały się całkowicie oderwane od rzeczywistych potrzeb i faktów. Właściwie nie ma obrony. I w związku z tym nie ma cyfrowego zaufania, zapomnijmy o *digital trust*.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 14 lutego 2023 r.