Stracone cyber-szanse

Niby cyberbezpieczeństwo jest na wszystkich sztandarach i wszyscy zapewniają o swoim zaangażowaniu w jego zapewnienie. Życie mocno jednak weryfikuje wypowiadane słowa i publikowane deklaracje, zaś decydenci nerwowo reagują na jakiekolwiek uwagi, które najczęściej odbierają jako nieuzasadnioną krytykę.

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

Moja Wspólnota Mieszkaniowa od lat dostarcza mi wiele mocnych wrażeń. Nie inaczej jest w tym roku. W marcu razem z zawiadomieniem o corocznym zebraniu ogółu członków wspólnoty otrzymałam projekt uchwały w sprawie elektronicznego głosowania uchwał Wspólnoty Mieszkaniowej o następującej treści:

§ 1. Właściciele wyrażają zgodę na możliwość głosowania uchwał Wspólnoty za pośrednictwem poczty elektronicznej, internetu bądź innych narzędzi internetowych, do których dostęp zadeklarują właściciele lokali we Wspólnocie.

§ 2. Elektroniczne głosowanie uchwał Wspólnoty może się odbywać jedynie na podstawie wcześniej zadeklarowanych adresów mailowych członków Wspólnoty lub ich pełnomocników.

Nie jestem przeciwna głosowaniom przez internet. Propozycję zarządu uznałam za niedopuszczalną, ponieważ do projektu uchwały nie był dołączony żaden regulamin lub inny dokument wyjaśniający, jak zaproponowany sposób głosowania zapewni ich prawidłowość, wiarygodność, autentyczność, uczciwość, integralność, niezaprzeczalność i rozliczalność oraz cyberbezpieczeństwo. Na szczęście kilku innych właścicieli wraz ze mną zagłosowało PRZECIW i proponowany sposób elektronicznego głosowania nie został przyjęty.

Największy udziałowiec był ZA. Spytałam go dlaczego. Odpowiedział mi na piśmie, że zgodnie z art. 60 Kodeksu Cywilnego *konieczne jest jedynie, aby oświadczenie głosującego członka wspólnoty przybrało formę ujawniającą jego wolę co do tego, w jaki sposób głosuje, w sposób dostateczny*. Stwierdził także, że zaproponowany sposób głosowania *nie wyklucza możliwości sprawdzenia przez każdego właściciela prawidłowości przeprowadzonego głosowania*. I dodał, że *głosowanie w sprawie inicjowanych uchwał odbywa się w sposób jawny, jednakże niezależny, a każdy z członków Wspólnoty może opowiedzieć się za takim rozwiązaniem sprawy, które jest w jego ocenie najbardziej słuszne*.

Poważnie? Na serio? Naprawdę zaproponowany sposób głosowania umożliwi sprawdzenie jego prawidłowości w sposób dostateczny? Rozpoznałam, czy w jednostce głównego udziałowca odbywają się głosowania w formie elektronicznej. Okazało się, że zamiast pełnej dowolności w składaniu oświadczenia woli stosowany jest system do głosowań przy użyciu urządzeń elektronicznych esesja.pl. Skontaktowałam się z producentem systemu i poprosiłam o informacje dotyczące zapewniania niezaprzeczalności, rozliczalności i cyberbezpieczeństwa. Zaskoczył mnie pozytywnie, przesyłając odpowiedź wskazującą na dochowywanie należytej staranności, kluczowej dla uczciwości wszystkich rodzajów i sposobów głosowania.

Niebezpieczna nieświadomość

Osoby, które praktycznie zajmują się bezpieczeństwem informacji, od razu rozpoznają, jak absurdalne jest powyższe podejście do głosowania przez internet. Laicy i prawnicy niekoniecznie. Niestety, nadal nie ma *jednolitego modelu edukowania obywateli na temat bezpieczeństwa w sieci oraz nie stworzono rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu „cyberhigieny"*. Jest to jeden z podstawowych wniosków kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości" przeprowadzonej przez Najwyższą Izbę Kontroli za okres 1.01.2019 – 31.12.2021 r.

Raport został opublikowany 7.03.2023 r. i jest dostępny na stronie https://www.nik.gov.pl/aktualnosci/przestepstwa-internetowe-zapobieganie-i-zwalczanie.html. Kontrolą objęto KPRM (jednostka obsługująca ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa), Komendę Główną Policji oraz NASK – PIB.

KPRM miała wiele zastrzeżeń do raportu. Przedstawiła je:

- w stanowisku Ministra Cyfryzacji do informacji o wynikach kontroli z dnia 16.12.2022 r., pisząc m.in.: *Celem ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa jest zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług,* ***nie zaś ochrona pojedynczych użytkowników Internetu.***

- w komentarzu KPRM Cyfryzacja z dnia 09.03.2023 r., pisząc m.in.: ***Kontrola****, której wyniki opublikowano 7 marca 2023 r. w raporcie NIK (…)* ***została przeprowadzona dwa lata temu****. Wnioski z niej nie obejmują zasadniczych zmian w obszarze legislacji ani podejmowanych działań, które zostały zintensyfikowane w ostatnim czasie. Zachęcamy więc do aktualizacji wiedzy i zapoznania się z inicjatywami Cyfryzacji KPRM oraz NASK – PIB, których celem jest poprawa cyberbezpieczeństwa, podniesienie kompetencji cyfrowych obywateli i budowanie bezpiecznej i stabilnej infrastruktury cyber. (…) przypominamy, że stworzenie jednego modelowego procesu edukacji w obszarze cyberzagrożeń byłoby nieskuteczne – należy dostosowywać komunikaty i treści do poszczególnych grup docelowych, uwzględniając przy tym szereg zmiennych: wiek, poziom kompetencji cyfrowych, sposób korzystania z internetu (aplikacje, gry komputerowe, fora internetowe, media społecznościowe, bankowość elektroniczna itd.). W zależności od odbiorcy budowana jest narracja i komunikacja, której celem jest uwrażliwienie użytkowników na cyberzagrożenia, edukowanie w zakresie cyberbezpieczeństwa, zabezpieczenia urządzeń, z których korzystają oraz umiejętności poruszania się w sieci.* ***Teza postawiona przez kontrolerów, że przekaz należy ujednolicić i niejako zamknąć w jednej przestrzeni (np. w jednym serwisie rządowym poświęconym tej tematyce) jest więc błędna i wynika – jak się wydaje – z nieznajomości badanego przez nich obszaru.***

Poważnie? Na serio? W artykule „Cyfrową maseczkę noś cały czas", opublikowanym w numerze 3/2022 kwartalnika „Domena", przytoczyłam wyniki badań opublikowane w 2022 r. przez różne instytucje finansowe, potwierdzające ustalenia NIK w zakresie braku wiedzy Polaków o cyberbezpieczeństwie. Jako wzór serwisu rządowego wskazałam zaś brytyjską stronę https://www.ncsc.gov.uk/ Równie inspirująca jest francuska strona rządowa https://www.cybermalveillance.gouv.fr/, która ma za zadanie wspierać **wszystkie ofiary cyberszkodliwych działań** i ułatwić im zgłaszanie incydentów.

Zachęcona przytoczonym komentarzem postanowiłam zweryfikować skuteczność inicjatyw Cyfryzacji KPRM oraz NASK – PIB, których celem jest podniesienie kompetencji cyfrowych obywateli. Przede wszystkim wykorzystałam wspólne posiedzenie Komisji Cyfryzacji, Innowacyjności

i Nowoczesnych Technologii i Komisji Spraw Zagranicznych, które odbyło się dwa dni po publikacji raportu NIK i dotyczyło przygotowania państwa na płynące z zagranicy zagrożenia związane z cyberprzestępczością. Zadałam przedstawicielowi KPRM kilka pytań w kwestii działań edukacyjnych i uświadamiających:

- Co by pan polecił woźnej w przedszkolu, która także korzysta z technologii, bo ma smartfona?
- Gdzie ma zajrzeć do internetu, żeby się dowiedzieć, jakie są zagrożenia przestępczością w internecie?
- Na co ma zwrócić uwagę? Z jakim materiałem się zapoznać?

Odpowiedź była dość zaskakująca: *na stronie gov.pl, czyli na naszej stronie rządowej, jest baza wiedzy o cyberbezpieczeństwie. Wystarczy wpisać „cyberbezpieczeństwo" na naszej stronie gov.pl. Wyświetli się bezpośrednie odniesienie do danych dotyczących cyberbezpieczeństwa. Tam jest cała baza wiedzy. Każdy aspekt wytłumaczony jest językiem ludzkim. Nie potrzeba mieć żadnej dodatkowej wiedzy technicznej, żeby zrozumieć kwestie, które tam są opracowane specjalnie dla każdego obywatela*. Czyli jest jednak możliwy ujednolicony przekaz zamknięty w jednej przestrzeni.

Pozostaje pytanie, ile osób, w tym ilu zawodowców, wie o wspomnianej bazie wiedzy. Nadal za mało. Dla przykładu: pod koniec marca br. odbyło się szkolenie online Wojewódzkiego Ośrodka Medycyny Pracy w Gdańsku na temat: „W jaki sposób w dzisiejszych czasach zapewnić cyberbezpieczeństwo danych zawartych w dokumentacji medycznej", adresowane do lekarzy, pielęgniarek i jednostek służby medycyny pracy w województwie pomorskim. Na koniec wykładu prelegent polecił pięć portali, które mogą zawierać przydatne informacje dotyczące cyberbezpieczeństwa. Tylko jeden z nich był rządowy – CERT Polska. Prelegent ani słowem nie wspomniał o bazie wiedzy.

Sprawdziłam także poradnik „Dobre praktyki cyberbezpieczeństwa w pracy adwokata i kancelarii", przyjęty i rekomendowany przez Naczelną Radę Adwokacką z dniem 16.01.2023 r. i dostępny na stronie https://www.adwokatura.pl/z-zycia-nra/dobre-praktyki-cyberbezpieczenstwa-w-pracy-adwokata-i-kancelarii/.

Materiał został przygotowany przez adwokatów działających w Instytucie LegalTech przy NRA. W dokumencie jest rekomendacja regularnego śledzenia aktualnych zaleceń instytucji zajmujących się tematyką cyberbezpieczeństwa (np. ENISA) ze względu na krótki cykl zmian technologicznych oraz wzrastający poziom cyberzagrożeń. Są podane tłumaczenia własne definicji zaczerpniętych z publikacji NIST:

– chmury obliczeniowej z „The NIST Definition of Cloud Computing", Special Publication 800-145,

– incydentu z „Guide for Security-Focused Configuration Management of Information Systems", Special Publication 800-128.

Pojawia się tajemniczy Administrator Systemu Informatycznego (ASI). Jest też zalecenie wdrożenia norm ISO z rodziny ISO/IEC 27000 w kancelariach małych (opcjonalnie), średnich i dużych, przy czym uzyskanie certyfikatu zgodności z normami ISO nie jest konieczne.

Wygląda na to, że autorzy nigdy nie słyszeli ani o bazie wiedzy, ani o Narodowych Standardach Cyberbezpieczeństwa czy Standardach Cyberbezpieczeństwa Chmur Obliczeniowych. Zalecają dokonanie zmapowania procesów i zabezpieczeń stosowanych wewnątrz własnej organizacji, a następnie – na podstawie rzetelnej **analizy ryzyka** – podjęcie decyzji w przedmiocie stosowania określonych środków technicznych i organizacyjnych. Na liście wymienionych norm z rodziny ISO/IEC 27000 (27000, 27001, 27002, 27017, 27018, 27032) zabrakło jednak normy ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. Jak zaznaczono w internetowym komunikacie, prace nad poradnikiem były prowadzone równolegle z pracami Naczelnej Rady

Adwokackiej nad udostępnieniem odpowiednich narzędzi technicznych i rozwojem elektronicznego Systemu Obsługi Adwokatury (e-SOA) na infrastrukturze Google. Zastanawiam się, jak przebiegło wdrożenie systemu zarządzania bezpieczeństwem informacji w NRA i jak wygląda jego stałe i konsekwentne stosowanie – co jest dużo większym wyzwaniem niż samo wdrożenie.

Niebezpieczne zaniedbania

Mija pięć lat stosowania RODO. Nadal pamiętam, jak w Polsce prawnicy całkowicie zdominowali temat wprowadzenia Rozporządzenia do firm i instytucji. Skoncentrowali się na tzw. klauzulach informacyjnych i politykach prywatności, zarabiając przy okazji ogromne pieniądze. Cyberbezpieczeństwo systemów przetwarzających dane osobowe było przez nich spychane na drugi, jeżeli nie na trzeci plan. Jakież było moje zdziwienie, gdy zapoznałam się z raportem LegalTech 2023 (https://legalis.pl/wp-content/uploads/2023/03/LTF_raport_2023.pdf) opublikowanym przez Wydawnictwo C.H.Beck. Szczególnie pikantne fragmenty cytuję w całości:

[str. 9] *Niewątpliwie ciekawą informacją jest to, że aż 1/3 prawników osobiście zetknęła się z próbami cyberataku. Widać także wyraźnie, że najmniej przygotowani do stawienia czoła zagrożeniom cyberbezpieczeństwa są prawnicy wykonujący zawód indywidualnie, co jest wskazówką dla samorządów odnośnie do kierunków edukacji w tym zakresie. Na tym tle zaskoczeniem jest wzrostowy trend liczby prawników korzystających z bezpłatnej poczty elektronicznej w chmurze. Oznacza to, że nadal wielu prawników nie rozumie, w jaki sposób działają bezpłatne usługi chmurowe oraz zapewne nie zdaje sobie sprawy z zagrożeń dla tajemnicy zawodowej. To wydaje się kolejnym ważnym zagadnieniem, na które trzeba zwrócić uwagę w edukacji prawników.*

[str. 19] *Kancelarie wdrażają wiele technologii w zakresie ochrony danych, ale mam wrażenie, że nadal robią to w sposób wybiórczy i chaotyczny, bez zdefiniowania strategii takich działań. Badania pokazują, że jesteśmy jako branża prawna nadal w procesie transformacji cyfrowej, szczególnie w obszarze technologii dotyczących cyberochrony. Trend jest pozytywny, niemniej jednak w porównaniu z innymi sektorami gospodarki mamy jeszcze wiele do zrobienia.*

[str. 23] *Zaprezentowany w badaniu poziom procentowy udziału w szkoleniach z zakresu cyberbezpieczeństwa nie jest optymistyczny, biorąc pod uwagę, że statystycznie najwięcej kancelarii w Polsce jest 1-, 2-, 3-osobowych. Zadaniem samorządów zawodowych powinno być więc popularyzowanie zagadnień związanych z tą tematyką w celu podniesienia świadomości w tym zakresie.*

Poważnie? Na serio? Po latach RODO-wej gorączki okazuje się, że sami prawnicy nie nadążają z cyfrową ochroną danych osobowych, nie znają zasad cyberhigieny i nie potrafią bezpiecznie stosować narzędzi informatycznych w swojej pracy. Sami z rozbrajającą szczerością przyznają, że nie radzą sobie z cyberbezpieczeństwem. Zaznaczam, że najwięcej administracyjnych kar pieniężnych Prezes UODO nakłada właśnie za brak stosowania się do zapisów art. 32 Bezpieczeństwo przetwarzania RODO.

> *Wniosek: warto zacząć nas słuchać, zamiast marginalizować nasze standardy, normy, metodyki i dobre praktyki czy traktować je fasadowo.*

Niebezpieczne morele

Skoro mowa o art. 32 RODO, zainteresowani mocno przeżywają wyrok Naczelnego Sądu Administracyjnego z dnia 9.02.2023 r. o sygnaturze akt III OSK 3945/21, uchylający zaskarżony wyrok WSA i zaskarżoną decyzję Prezesa UODO nakładającą na Morele.net Sp. z o.o. administracyjną karę pieniężną w wysokości 2 830 410 PLN (660 000 EUR). Szczególnie zbulwersowały ich następujące zapisy z uzasadnienia wyroku: ***(…) należy podać w wątpliwość, czy organ*** *[UODO] – w dacie wydania zaskarżonej decyzji –* ***posiadał własną wiedzę specjalistyczną****, pozwalającą na ocenę odpowiedniości środków technicznych i organizacyjnych w działalności gospodarczej [Morele.net] o tak dużej skali. W ocenie Sądu kasacyjnego o posiadaniu takiej wiedzy specjalistycznej,* ***niezbędnej do zastąpienia opinii biegłego własnymi ustaleniami****, nie przesądza samo twierdzenie organu administracji.* ***Organ*** ten ***powinien być w stanie uprawdopodobnić, iż w rzeczywistości posiada wiedzę****, która nie tylko subiektywnie, ale i obiektywnie, a więc z zachowaniem wymaganej przez art. 8 § 1 k.p.a. bezstronności, pozwoli na dokonanie wymagającej wiedzy specjalistycznej oceny okoliczności sprawy… Jakkolwiek w sprawie nie ma podstaw do podważania wiedzy specjalistycznej pracowników Urzędu Ochrony Danych Osobowych, to* ***wątpliwe wydaje się, czy organ w swojej dotychczasowej praktyce prowadził postępowania w zbliżonej kategorii spraw, co pozwalałoby na ustalenie odpowiedniego do charakteru, zakresu i kontekstu przetwarzania standardu środków bezpieczeństwa****. Wniosek ten wzmacnia fakt, iż do wycieku danych osobowych doszło w październiku 2018 r., a więc niedługo po wejściu w życie RODO. Prowadząc postępowanie administracyjne i wydając we wrześniu 2019 r. decyzję o nałożeniu kary pieniężnej,* ***Prezes UODO rozstrzygał sprawę w oparciu o nowy stan prawny. Organ nie mógł skutecznie powołać się na wiedzę specjalistyczną pracowników urzędu, skoro odnosiła się ona do poprzedniego stanu prawnego, w ramach którego nie stosowano rozwiązania takiego jak w art. 32 RODO, polegającego na niedookreśleniu odpowiedniego standardu wymaganych środków technicznych.*** *Za* ***nieprzekonujące*** *Naczelny Sąd Administracyjny uznaje zawarte w odpowiedzi na skargę kasacyjną wyjaśnienia, iż model ochrony danych osobowych oparty na założeniu, że przyjmo-*

wane przez administratorów środki powinny być dostosowane do zagrożeń i charakteru przetwarzanych danych nie jest nowością, a Generalny Inspektor Ochrony Danych Osobowych niejednokrotnie identyfikował zagrożenia i zobowiązywał administratorów w formie decyzji administracyjnych do wdrożenia środków adekwatnych do ryzyka. Okoliczności te pozostają bez znaczenia dla sprawy, zważywszy na skalę działalności M. i związaną z nią ***specyfikę stosowanych środków zabezpieczenia*** *danych osobowych ponad dwóch milionów klientów.*

Prezes UODO uznał, że orzeczenie NSA w sposób niezaprzeczalny i precedensowy zarówno kwestionuje jego niezależność jako organu nadzorczego, jak i podważa jego kompetencje oraz kwalifikacje merytoryczne zatrudnionych w nim osób, niezbędne do wykonywania zadań, do których organ ten został powołany. Wydał komunikat, który do tej pory jest na pierwszym miejscu na stronie Urzędu, wystosował list otwarty do Prezesa NSA, zorganizował naprędce konferencję „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów" i poruszył sprawę w dwóch artykułach w nr 2/04/2023 swojego biuletynu. Przy okazji dowiedzieliśmy się, że *personel Urzędu ma* ***blisko dwudziestopięcioletnie doświadczenie*** *w kontroli i prowadzeniu postępowań wobec podmiotów przetwarzających dane osobowe w systemach informatycznych, które to* ***doświadczenie jest systematycznie wzbogacane****, przez co w tym okresie wytworzona została* ***unikalna wiedza instytucjonalna*** *organu, dająca gwarancję posiadania wiedzy specjalistycznej pozwalającej na samodzielną ocenę stosowania środków technicznych i organizacyjnych w systemach informatycznych bez konieczności korzystania z pomocy biegłego*.

Poważnie? Na serio? Unikalna wiedza instytucjonalna w zakresie cyberbezpieczeństwa? Zajrzałam do sprawozdań z działalności Prezesa UODO w latach 2010–2021 (nie ma jeszcze sprawozdania za 2022 r.) i sprawdziłam zatrudnienie ogółem oraz w Departamencie Informatyki (DIF). Oto liczba etatów v. liczba osób w DIF na koniec danego roku:

2010 – 120/14	2016 – 145,73/10
2011 – 126,9/15	2017 – 150,53/10
2012 – 126,48/15	2018 – 161,65/13
2013 – 122,36/15	2019 – 231,25/10
2014 – 129,86/15	2020 – 244,05/11 (10,42 etatu)
2015 – 126,105/15	2021 – 270/8 (7,42 etatu)

Liczba spraw rośnie, liczba etatów rośnie, a liczba informatyków maleje. Może są w Departamencie Kontroli i Naruszeń, który w zeszłym roku rekrutował specjalistów ds. informatycznych i kontroli? Ich obowiązkiem ma być m.in. ocena rozwiązań technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych. Wśród wymagań była wiedza i doświadczenie z zakresu bezpieczeństwa teleinformatycznego, umiejętność analitycznego myślenia i przynajmniej roczny staż pracy. Dopiero w dodatkowych atutach wymieniono m.in. doświadczenie w zarządzaniu bezpieczeństwem informacji i znajomość zagadnień związanych z cyberbezpieczeństwem. Ja dołączam skan mojego certyfikatu CISA do każdej umowy lub raportu z audytu dla potwierdzenia mojej wiarygodności i moich kompetencji. Liczę, że w sprawozdaniu za 2022 r. znajdą się szczegółowe informacje dotyczące specjalistycznych kursów i szkoleń zaliczonych przez pracowników UODO, dokumentujące ich znajomość środków bezpieczeństwa wymaganych w systemach informatycznych w celu zapewnienia odpowiedniego poziomu ochrony danych osobowych.

Niebezpieczny Niebezpiecznik

Na koniec apel do portalu Niebezpiecznik.pl. 19 kwietnia br. na konferencji z okazji 5 lat RODO kolejny raz pracownik portalu namawiał słuchaczy do zgłaszania zauważonych incydentów dotyczących cyberbezpieczeństwa i naruszeń ochrony danych osobowych bezpośrednio do redakcji portalu z pominięciem właściwych podmiotów, w tym organizatora imprezy. Wzywam portal do zaprzestania opisanej praktyki. Jeżeli ktokolwiek zauważy jakikolwiek incydent czy jakiekolwiek naruszenie, to przypominam, że jest kilka opcji ich zgłoszenia:

- do podmiotu, którego dotyczy incydent lub naruszenie,
- na policję,
- do CERT.pl,
- do jednego z zespołów CSIRT,
- do odpowiedniego urzędu (UODO, UKE, inne).

Nie zgadzam się na utrzymywanie drugiego obiegu informacji poza krajowym systemem cyberbezpieczeństwa budowanym przez nas z dużym mozołem.

Pracownik portalu poinformował także, że portal pomaga za darmo podmiotom, których dotyczy incydent lub naruszenie. Pozostaje pytanie, jaka jest odpowiedzialność portalu za świadczone „koleżeńskie" wsparcie.

9.05.2023 r. Ministerstwo Cyfryzacji poinformowało m.in. o zeszłorocznym badaniu świadomości Polek i Polaków z zakresu cyberbezpieczeństwa przeprowadzonym dla Google przez CBM Indicator, które wykazało, że o phishingu słyszało 47% ankietowanych, o ataku DDoS 21%, a o ataku ransomware zaledwie 16%. Tym samym Ministerstwo potwierdziło, że przegapiono i stracono wiele szans na podniesienie ogólnego poziomu cyberbezpieczeństwa. RODO jest tego dobitnym przykładem. Nie warto się obrażać na niezależne weryfikacje i oceny działań podejmowanych przez poszczególne podmioty. Lepiej je przeanalizować i wykorzystać w codziennej pracy na rzecz bezpieczeństwa Polaków w sieci.

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