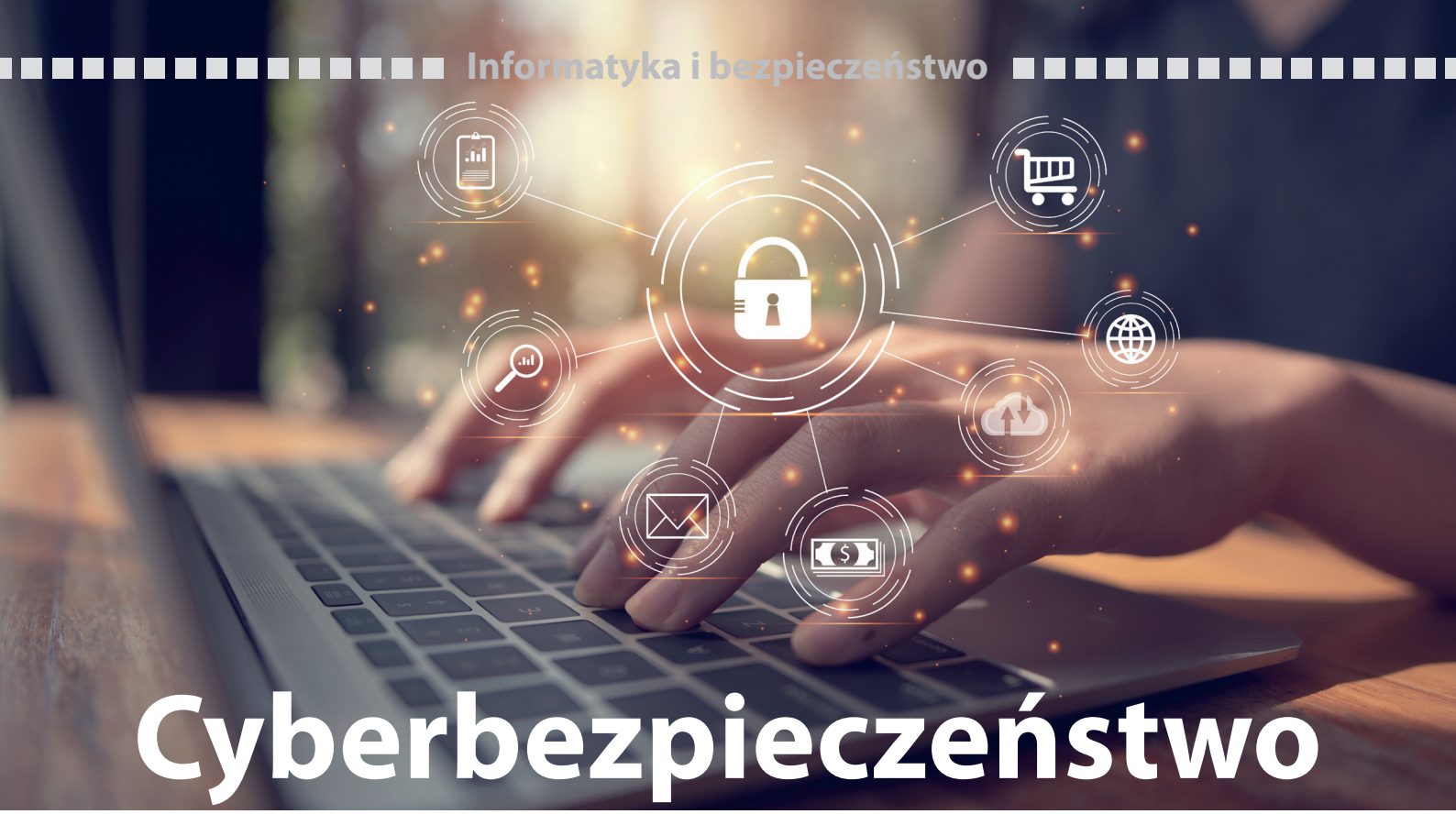


Cyberbezpieczeństwo po amerykańsku

Wbrew tytułowi artykuł nie dotyczy cyberbezpieczeństwa w USA. Przedstawia moją opinię na temat przydatności Narodowych Standardów Cyberbezpieczeństwa (NSC), przedstawianych jako zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych, wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji.

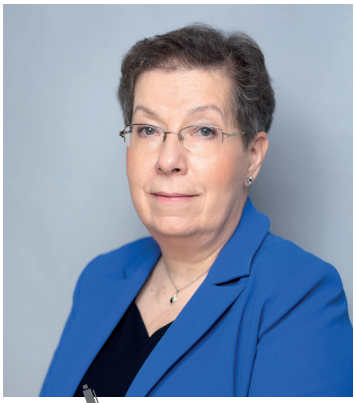
NSC wprowadził Pełnomocnik Rządu ds. Cyberbezpieczeństwa z dniem 1 września 2021 r. w ramach realizacji interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 w zakresie opracowania i wdrożenia Narodowych Standardów Cyberbezpieczeństwa.

Z NSC można się zapoznać na stronie: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber.

Made in USA

Jestem fanką amerykańskich standardów, wytycznych i dobrych praktyk dotyczących bezpieczeństwa informacji. Amerykanie w swoich opracowaniach piszą wprost, co warto zrobić i na co należy zwracać uwagę. Nawet Brytyjczycy czy Australijczycy (też Anglosasi) nie są tak bezpośredni.

Narodowe Standardy Cyberbezpieczeństwa to przetłumaczone wybrane publikacje National Institute of Standards and Technology (NIST), z których jako „godnych zaufania" korzystamy od lat. Należy jednak pamiętać, że są to standardy i wytyczne opracowane w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych **administracji federalnej USA**, której nie da się porównać



Joanna Karczewska
One of Europe's Top Cyber Women

z naszą administracją rządową i samorządową. Wprawdzie Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów zarzeka się, że standardy posiadają mapowanie na obowiązujące w naszym systemie prawnym Polskie Normy, ale samo mapowanie nie wystarczy, co pokażę na przykładach.

13 czy 17

Dyrektywa NIS wymaga od operatorów usług kluczowych i dostawców usług cyfrowych uwzględniania najnowszego stanu wiedzy w zakresie bezpieczeństwa sieci i systemów informatycznych. Popatrzmy na „Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013" (standard NSC 800-53 MAP wer. 1.0). Tu pojawia się pierwszy zgrzyt. Jak wynika z informacji umieszczonej na stronie Polskiego Komitetu Normalizacyjnego, odpowiednia polska norma PN-ISO/IEC 27001:2014-12 została wycofana i zastąpiona normą PN-ISO/IEC 27001: 2017-06. Dlaczego więc Narodowy Standard Cyberbezpieczeństwa wydany w 2021 r. nie uwzględnia zmiany normy dokonanej w 2017 r.?

Od lat uczestniczę w pracach nad metodyką COBIT i innymi dokumentami publikowanymi przez stowarzyszenie ISACA, którego jestem członkiem. Pamiętając jednakże o różnicach kulturowych i prawnych, staram się przekładać standardy amerykańskie na polskie realia. Stąd m.in. moje dwa uznane opracowania (nadal do znalezienia w Internecie):

- **wytyczna „UODO Survival Kit" z 2005 r., przygotowana razem z Mirosławem Błaszczakiem, Piotrem Dzwonkowskim i Sebastianem Łatasiem;**
- **„Mapowanie minimalnych wymagań dla systemów teleinformatycznych używanych przez podmioty realizujące zadania publiczne na COBIT 5" z 2013 r., przygotowane razem z Wojciechem Szyszką i Łukaszem Wilkoszem.**

Ukoronowaniem moich starań popularyzatorskich było wykorzystanie metodyki COBIT w trakcie kontroli „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych", przeprowadzonej przez Najwyższą Izbę Kontroli w 2015 r. Miałam zaszczyt doradzać Izbie, jak za pomocą metodyki dokonać oceny poziomu zarządzania procesem „Zapewnienie bezpieczeństwa systemów informatycznych" w wybranych instytucjach administrujących systemami informatycznymi, służącymi do realizacji istotnych zadań publicznych.

Drugi zgrzyt dotyczy określenia „polityka", czyli angielskiego słowa „policy". Od lat posługujemy się pojęciem „polityka" w odniesieniu do regulacji wewnętrznych zatwierdzonych przez kierownictwo, zawierających opis podstawowych zasad oraz środków technicznych i organizacyjnych przyjętych w organizacji dla zapewnienia poufności, integralności i rozliczalności przetwarzanych informacji i danych osobowych. Norma PN-ISO/IEC 27001:2014-12 wręcz wymaga ustanowienia przez najwyższe kierownictwo **polityki** bezpieczeństwa informacji i komunikowania jej znaczenia. Dlatego nie rozumiem tłumaczenia „policies" jako „zasady" we wszystkich publikowanych NSC (z nielicznymi wyjątkami), chociaż w NSC 800-53 MAP zabezpieczenie „AC-1 POLITYKA I PROCEDURY" jest zestawione z punktem „5.2 Polityka" normy 27001.

Znowu od zera

Gdy zobaczyłam listę przetłumaczonych NSC, od razu pomyślałam – znowu zaczynamy od zera. Mamy odłożyć „stare zabawki" na rzecz nowych „przewodników metodycznych". Skoro tak, to należą nam się wyjaśnienia dotyczące kilku kluczowych kwestii:

1. **NSC 200 a Rozporządzenie o KRI**

   Czy NSC 200 wer. 2.0 „Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych" ma zastąpić rozporządzenie o KRI obowiązujące od 12 kwietnia 2012 r.? Zgodnie z rozporządzeniem, kierownictwo podmiotu publicznego jest zobowiązane do zapewnienia warunków umożliwiających realizację i egzekwowanie minimalnych wymagań dotyczących systemu zarządzania bezpieczeństwem informacji zawartych w § 20 ust. 2. NIK zdążyła już wielokrotnie zbadać stopień wdrożenia i stosowania tych wymagań. Jej raporty wskazują, że nadal nie jest najlepiej. Czy zatem NSC 200 ma być panaceum na trwające już 10 lat trudności w realizacji i egzekwowaniu bezpieczeństwa systemów informatycznych? Czy standard będzie lepiej „wspierać rozwój, wdrażanie i funkcjonowanie bezpieczniejszych systemów informatycznych"? Przydałoby się także wzajemne mapowanie obu zestawów minimalnych wymagań.

2. **NSC 800-37 a inne metodyki zarządzania ryzykiem**

   Czy NSC 800-37 „Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu" ma zastąpić wszelkie dotychczas opracowane i stosowane przez nas metodyki zarządzania ryzykiem? Są to m.in.:

   - „Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych", opracowana przez Ministerstwo Administracji i Cyfryzacji i przyjęta w dniu 12 listopada 2015 r. przez Komitet Rady

Ministrów ds. Cyfryzacji, który rekomenduje administracji rządowej jej stosowanie;

- dwuczęściowy poradnik Prezesa Urzędu Ochrony Danych Osobowych zatytułowany „Jak rozumieć podejście oparte na ryzyku według RODO?" i „Jak stosować podejście oparte na ryzyku?", w którym przedstawione zostały kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka, czyli tzw. oceny skutków dla ochrony danych;

- „Analyse d'impact relative à la protection des données" (AIPD), opracowana przez francuski organ nadzorczy CNIL i przetłumaczona przeze mnie na język polski.

Przywołuję metodyki zarządzania ryzykiem dotyczące ochrony danych osobowych, ponieważ przetłumaczony NSC 800-37 wersja 2 z 2018 r. zawiera mnóstwo odniesień do prywatności oraz Personally Identifiable Information, w skrócie PII – po naszemu – do danych osobowych. Stanowi odpowiedź NIST na europejskie RODO. Tłumacze najwyraźniej nie wiedzieli o tym i na siłę uzupełnili standard o dopiski dotyczące danych osobowych, na dodatek zostawiając skrót PII w kilku miejscach.

3. NSC a szablony audytu zgodności z uksc

Czy nadal obowiązują opublikowane w kwietniu 2020 r. szablony sprawozdania z Audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa? Czy szablony zostaną dopasowane do NSC? Czy obecnie wymagane przez uksc audyty bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej powinny obejmować badanie zgodności z Narodowymi Standardami Cyberbezpieczeństwa? Szablony zawierają dość ogólne odniesienia do zapisów normy PN-EN ISO/IEC 27001 w zakresie wymagań stawianych systemowi zarządzania bezpieczeństwem informacji. Można skorzystać z NSC 800-53 MAP, ale przydałyby się dodatkowe wyjaśnienia.

4. NSC a Diagnoza Cyberbezpieczeństwa

Czy zmianie ulegnie Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa JST? Diagnoza jest obligatoryjna dla rozliczenia grantu przyznanego w ramach programu Cyfrowa Gmina, ogłoszonego we wrześniu 2021 r. (po dacie publikacji NSC). Formularz obejmuje ocenę zgodności z rozporządzeniem o KRI i ustawą o ksc. Czy gminy powinny także sprawdzać zgodność z NSC 200?

Made in Poland

Tłumaczenie amerykańskiego tekstu technicznego jest równie trudne co przekład książek o Harrym Potterze. Na tłumaczy czyhają tysiące pułapek, nie tylko w postaci Dobby'ego/Zgredka. Błędne tłumaczenie może rozbawić specjalistę, a laika zwieść. Porównałam wersję amerykańską i polską standardu NSC 200 oraz NSC 800-61, który mnie szczególnie zainteresował, bo jako jedyny został dodatkowo zweryfikowany przez cyberbezpieczników. Oto co wykazała analiza:

1. Brak konsekwencji w adaptacji NSC do polskich realiów

Jak wynika z porównania, tłumacze pokusili się o różne modyfikacje, pominięcia i uzupełnienia, by „spolonizować" standardy. Niestety, nie byłam w stanie rozpracować, jaki przyjęli klucz. Nie rozumiem, dlaczego fragment o treści: *Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are likely to leverage in their social engineering* zamieniono na: *Zalecenia są często najbardziej potrzebne, gdy pojawiają się nowe zagrożenia, takie jak ataki typu phishing np. z zainfekowanymi plikami pdf (pseudo faktury)*. Przecież u nas ataki z wykorzystaniem celebrytów czy wydarzeń politycznych też się zdarzają. Natomiast bez zmian pozostawiono scenariusz obsługi incydentu nr 3, który mnie wyjątkowo rozbawił.

Scenariusz obsługi incydentu nr 3: Skradzione dokumenty

W poniedziałek rano dział prawny organizacji odbiera telefon z organu ścigania w sprawie podejrzanej działalności związanej z systemami organizacji. Później tego samego dnia funkcjonariusz organu ścigania spotyka się z członkami zarządu i działem prawnym, aby omówić tę działalność. Organ ścigania prowadzi dochodzenie w sprawie publicznego opublikowania poufnych dokumentów rządowych, a niektóre dokumenty podobno należą do organizacji. Funkcjonariusz prosi organizację o wsparcie, a kierownictwo prosi zespół reagowania na incydenty o pomoc w uzyskaniu niezbędnych dowodów w celu ustalenia, czy te dokumenty są legalne, czy nie, oraz w jaki sposób mogły zostać ujawnione.

2. Brak znajomości amerykańskiego języka technicznego

Przy mechanicznym tłumaczeniu pojawiają się zabawne potworki językowe (ang. „gibberish"), np.:

- statement of management commitment – oświadczenie o zaangażowaniu w zarządzanie;

- images of clean OS and application installations – obrazy „czystego": systemu operacyjnego i instalacji aplikacji;

- hosts should have auditing enabled – hosty powinny mieć włączone przeprowadzanie audytu;
- affected external parties – dotknięte podmioty zewnętrzne;
- non-networked systems – systemy niezwiązane z siecią;
- real-time blacklists – czarne listy czasu rzeczywistego;
- well-connected employee – dobrze skomunikowany pracownik;
- specific impact information about incidents – szczegółowe informacje o wpływie na incydenty;
- organizational information systems – organizacyjne systemy informatyczne;
- monitor information system security alerts and advisories and take appropriate actions in response – monitorować ostrzeżenia i porady systemu informatycznego oraz w odpowiedzi na to podejmować odpowiednie działania.

3. **Brak znajomości pojęć dotyczących cyberbezpieczeństwa (i nie tylko) oraz brak spójności w stosowaniu przyjętych polskich odpowiedników**

   Nawet jeżeli pojęcie jest zawarte w NSC 7298 Słowniku kluczowych pojęć z zakresu cyberbezpieczeństwa, to nie oznacza, że polskie tłumaczenie jest właściwe. Dla przykładu:

   - controls – przetłumaczone jako środki/zabezpieczenia, nam znane są od lat jako mechanizmy kontrolne;
   - compromise (rzeczownik) – naruszenie (w Słowniku i tekście), złamanie, włamanie (w tekście);
   - compromise (czasownik) – zagrażać, złamać zabezpieczenia (w tekście);
   - compromised (przymiotnik) – naruszony, zagrożony, zaatakowany, którego dotyczy luka, zainfekowany (w tekście);
   - incident indicator – wskaźnik incydentu, który w Słowniku jest opisany jako oznaka, że incydent mógł wystąpić lub może aktualnie występować; zatem objaw, oznaka czy symptom byłyby właściwszym odpowiednikiem (szczególnie w kontekście incydentu);
   - policies – zasady, polityki, reguły (użyto wszystkich trzech słów w jednym dokumencie);
   - public affairs office – biuro spraw publicznych organizacji (chyba chodzi o rzecznika prasowego);
   - legal staff – personel prawny, dział prawny (zdecydowanie tylko to drugie).

Dobre rady Wujka Sama

NSC są pełne dobrych rad. Czy jesteśmy przygotowani na tak pragmatyczne podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności? Oto kilka kolejnych przykładów z NSC 800-61:

1. W punkcie 3.1.1. jest zapis: *Sposoby zgłaszania incydentów, takie jak numery telefonów, adresy e-mail, formularze online i bezpieczne systemy komunikatorów internetowych, których użytkownicy mogą używać do zgłaszania podejrzanych incydentów. Co najmniej jeden mechanizm powinien umożliwiać anonimowe zgłaszanie incydentów.* Sprawdziłam strony https://www.gov.pl oraz https://www.amw.gdynia.pl/. Nie znalazłam zalecanego mechanizmu.

2. W punkcie 3.2.4. jest zalecenie ustanowienia zasad retencji dzienników. Jak zaznaczono: *Tworzenie i wdrażanie zasad retencji dzienników, które określają, jak długo należy przechowywać dane dzienniki, może być niezwykle pomocne w analizie, ponieważ starsze wpisy dziennika mogą wskazywać na aktywność rozpoznania lub wcześniejsze wystąpienia podobnych ataków*. Warto przypomnieć, że wymogi dotyczące przechowywania zapisów dzienników systemów (logów) są określone w § 21 ust. 4 Rozporządzenia o KRI.

3. W punkcie 3.2.4. jest także zalecenie utrzymywania synchronizacji zegarów wszystkich hostów. Warto zaznaczyć, że Główny Urząd Miar udostępnia poprzez Internet usługę umożliwiającą synchronizację czasu w systemach komputerowych z czasem urzędowym obowiązującym w Polsce. Serwery czasu znajdują się w Głównym Urzędzie Miar, w Laboratorium Czasu i Częstotliwości. Są one synchronizowane z państwowego wzorca jednostek miar czasu i częstotliwości. Usługa jest dostępna całodobowo i bezpłatnie. Sama z niej korzystam na moich komputerach.

4. W punkcie 2.4.3., dotyczącym personelu reagowania na incydent [sic!] (ang. *Incident Response Personnel*), zaleca się, by każdy członek zespołu miał dobre umiejętności rozwiązywania problemów i umiejętność krytycznego myślenia (ang. *critical thinking*). Przejrzałam aktualne oferty pracy dla cyberbezpieczników. Nie znalazłam żadnego ogłoszenia, które by wymagało od kandydata krytycznego myślenia.

Podsumowanie

Każdy zestaw dobrych praktyk, który pomoże w zapewnianiu cyberbezpieczeństwa, jest wyczekiwany i pożądany. Byłabym jednak ostrożna w twierdzeniu, że korzystając z Narodowych Standardów Cyberbezpieczeństwa można **STOSUNKOWO ŁATWO** zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę. Mamy takie przysłowie: Bez pracy nie ma kołaczy.

Na standardy NSC składają się następujące opracowania (materiały do pobrania na stronie https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber):

- Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0)
- Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0)
- Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0)
- Poradnik Planowania Awaryjnego (NSC 800-34 wer. 1.0)
- Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0)
- Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0)
- Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0)
- Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0)
- Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0)
- Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0)
- Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część II (NSC 800-60 cz. 2 wer. 1.0)
- Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer. 1.0)
- Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" (NSC 800-207 wer. 1.0)
- Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (NSC 7298 wer. 1.0)

Miałam rację

W dniu ochrony danych w 2018 r., na Stadionie Narodowym, w trakcie konferencji o znamiennym tytule „Zainwestuj w prywatność. Przygotowujemy się do RODO", spytałam przedstawicieli GIODO o prawa internautów, dotyczące ich danych zbieranych za pomocą narzędzia Google Analytics używanego na stronie GIODO. Odpowiedź była krótka i lakoniczna: mam sobie sama to wyjaśniać z Google. Cztery lata później, w dniu ochrony danych w 2022 r., sprawdziłam stronę UODO. Google Analytics już nie jest używane. Miałam rację, sygnalizując problem. Swoją drogą ciekawe, co się stało ze zgromadzonymi przez lata danymi o naszych wizytach na stronie urzędu.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 16 lutego 2022 r.