PROTOKÓŁ z XXIII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 20 grudnia 2024 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

Otwarcie Posiedzenia – p. Agnieszka Jankowska, Przewodnicząca Rady ds. Cyfryzacji.

Pani Przewodnicząca powitała obecnych członków Rady ds. Cyfryzacji oraz zaproszonych na posiedzenie gości. Poinformowała, że podczas posiedzenia omówiony zostanie także temat projektu ustawy o Krajowym Systemie Certyfikacji Cyberbezpieczeństwa.

Certyfikacja w zakresie cyberbezpieczeństwa z perspektywy małych i średnich przedsiębiorstw – Pan Krzysztof Silicki, członek Rady ds. Cyfryzacji; Pan Paweł Kostkiewicz, Dyrektor Ośrodka Standaryzacji i Certyfikacji w NASK; Pani Marianna Sidoroff, Dyrektor Departamentu Gospodarki Cyfrowej w Ministerstwie Rozwoju i Technologii.

Pan Dyrektor Łukasz Wojewoda przedstawił prezentacje dot. projektu ustawy o Krajowym Systemie Certyfikacji Cyberbezpieczeństwa. Główne założenie projektu ustawy KSCC to certyfikacja jako dobrowolne przedsięwzięcie. Obok programów europejskich wprowadzone zostaną krajowe schematy certyfikacji. Minister Cyfryzacji będzie organem nadzorczym nad procesem. Ponadto, założeniem jest także zachęcanie podmiotów prywatnych do budowania zdolności do certyfikacji. Pan Dyrektor wskazał, że w schematach europejskich 3 elementy podlegają certyfikacji: produkty, usługi, procesy. Krajowy schemat zostanie rozszerzony o osoby i system zarządzania cyberbezpieczeństwem. Dokładane są starania, aby element ochrony osób był bardzo istotny w krajowym podejściu.

Krajowe schematy certyfikacji zostaną przyjęte jako rozporządzenia wydawane przez Ministra Cyfryzacji w pięcioletnim okresie z możliwością przedłużenia. Certyfikaty będą określać szczegółowe wymogi, które należy spełnić, aby otrzymać dany certyfikat. Minister Cyfryzacji będzie zdolny przede wszystkim do sprawowania nadzoru nad podmiotami obecnymi w procesie; wyrażania zgody w uzyskiwaniu certyfikatów na poziomie uzasadnienia zaufania; prowadzenia postępowań w sprawie zezwolenia na wykonywanie określonych działań w przypadku, gdy dany europejski program certyfikacji cyberbezpieczeństwa tego wymaga; współpracy z instytucjami UE oraz przygotowania krajowych schematów certyfikacji cyberbezpieczeństwa.

Pan Dyrektor przedstawił podział nadzoru nad Krajowym Systemem Certyfikacji – w PCA pozostaje akredytacja jednostki oceniającej zgodność oraz monitorowanie spełnienia wymagań akredytacyjnych. Projekt ustawy KSCC znajduje się obecnie na etapie Komitetu ds. Europejskich, a kolejnym etapem będzie Stały Komitet Rady Ministrów. Pan Dyrektor zwrócił uwagę na ostatnie zmiany w projekcie ustawy. W związku z tym, że przy wykonywaniu zadań MC z zakresu nadzoru nad certyfikacją są też Państwowe Instytuty Badawcze, mające możliwość wspierania Ministra Cyfryzacji, doprecyzowano w jaki sposób kompetencje, które mogłyby powodować ewentualny konflikt interesów są rozdzielone. Zostało wskazane

wprost, że te zadania nie będą mogły być realizowane przez tę samą komórkę organizacyjną w MC, a także wymienione, iż Państwowy Instytut Badawczy nie może wspierać Ministra Cyfryzacji w wykonywaniu jego zadań w przypadku, gdy uczestniczy w procesie certyfikacji.

Pan Dyrektor Paweł Kostkiewicz wskazał, że certyfikacja to fragment tzw. oceny zgodności przedmiotu z normami/standardami. Kluczową rolę pełni Polskie Centrum Akredytacji, które sprawdza laboratoria/jednostki certyfikujące, by zachowywały pewien dobry poziom - rzetelność, poufność, bezstronność. Pan Dyrektor zwrócił uwagę, że zaletą systemu akredytacji jest to, że każdy kraj europejski mając do dyspozycji takie samo narzędzie akredytuje na tych samych zasadach jednostki certyfikujące/laboratoria/jednostki audytorskie – certyfikat wystawiony przez NASK w jednostce certyfikującej ma tą samą rangę/wartość, co wystawiony przez jednostkę certyfikującą w innym kraju europejskim.

Pan Dyrektor wymienił, że certyfikować można produkty, usługi, procesy, systemy zarządzania, a także kompetencje. Certyfikacja czy ocena zgodności jest po to, by rynek działał lepiej jakościowo i bardziej wiarygodnie. Ocena zgodności może kończyć się dwoma typami zdarzeń – pierwszym jest umieszczenie znaku CE, któremu towarzyszy tzw. deklaracja zgodności, drugi, to znak certyfikacji. W zakresie certyfikacji systemów zarządzania jest obecnie 14 podmiotów/różnych jednostek certyfikujących - w większości prywatnych, w pewnej mierze niepolskich (tzn. filie dużych koncernów międzynarodowych mających w Polsce swoje lokalne siedziby), są także polskie miejsca. Ze względu na cyberbezpieczeństwo, Pan Dyrektor podzielił je na dwie grupy: systemy zarządzania bezpieczeństwem informacji oraz systemy zarządzania ciągłością działania. Od momentu kiedy pojawił się projekt ustawy o KSC, gdzie znalazła się wzmianka o potrzebie dowodzenia o dobrze zorganizowanej ciągłości działania w przedsiębiorstwie, liczba jednostek certyfikujących systemy zarządzania ciągłością działania wzrosła z 1 do 5. Istnieje też kilka jednostek certyfikujących osoby – przede wszystkim audytor wiodący do systemów zarządzania bezpieczeństwem informacji jak i ciągłości działania - to główna kompetencja, która dziś bywa certyfikowana. Pan Dyrektor wspomniał także o jednostce certyfikującej wyroby – jest to jednostka NASKu oraz o trzech Laboratoriach - największe posiada Instytut Łączności, EMAG porównywalnej wielkości oraz NASK ma laboratorium mniejsze przeznaczone głównie dla IOT. Jako system - zbiór laboratoriów i jednostka certyfikująca - Polska ma najszerszą dostępną akredytację.

W dalszej części wypowiedzi, Pan Dyrektor przedstawił także kontekst europejski i światowy. W Europie zjawisko jest znane od 1992 r. tzn. od tego czasu istnieje porozumienie SOG-IS MRA pomiędzy kilkoma krajami, które nawzajem uznają sobie certyfikaty. Polska jest w porozumieniu od 2017 r. Od 2024 r. mamy pierwszy europejski program certyfikacji oparty o normy Common Criteria. Na świecie obowiązuje porozumienie, które sięga szerzej - CRA. Pan Dyrektor wspomniał, że ocena zgodności to bezstronne i kompleksowe sprawdzenie poziomu bezpieczeństwa komponentów tworzących systemy IT w podmiotach kluczowych i ważnych w krajowym systemie cyberbezpieczeństwa: produktów usług, procesów, systemów zarządzania bezpieczeństwem informacji, systemów zarządzania ciągłością działania, kompetencji personelu.

Ponadto, Pan Dyrektor przedstawił plany rozwoju na najbliższe lata - zajęcie się zagadnieniem EU ID WALLET – europejskiego portfela tożsamości, wdrożeniem systemu certyfikacji osób wg ENISA Cybersecurity Skills Framework (ECSF). Kolejny obszar to dualuse – certyfikacja urządzeń i oprogramowania podwójnego stosowania, certyfikacja urządzeń wykorzystujących mechanizmy kryptografii kwantowej (QKD), oceny zgodności i certyfikacji AI zgodnie z AI Act, rozwój programu certyfikacji „Firma Bezpieczna Cyfrowo"- rozwiązania dla MŚP.

Pani Dyrektor Marianna Sidoroff wspomniała, że z jednej strony małe i średnie przedsiębiorstwa mają ogromne możliwości funkcjonowania w cyfrowości, jednak wyniki badań świadczą, że odstają od innych. Poszukiwano kompetencji, która szeroko i płasko spowoduje, że przedsiębiorcy skorzystają najwięcej na cyfryzacji - cyberbezpieczeństwo wydało się naturalną i oczywistą kompetencją. Mnóstwo czasu poświęcono na odkrycie w jaki sposób przekonać małych i średnich przedsiębiorców, w jaki sposób ich zbadać, co zrobić by wydzielić mikro oraz małych i średnich przedsiębiorców, którzy mają już pierwsze oprogramowanie. Dla MRiT „Firma Bezpieczna Cyfrowo" i certyfikacja firm jest jednym z elementów wielu działań, które przekładają się na transformację cyfrową przedsiębiorców. Przedsiębiorca może zacząć od autodiagnozy, by zobaczyć w jakim miejscu się znajduje na mapie wymagań cyberbezpieczeństwa, a także na mapie dojrzałości usług cyfrowych, które ma w swoim przedsiębiorstwie. Dzięki tej diagnozie pobiera spersonalizowany raport – plan działania. Pan Dyrektor P. Kostkiewicz wyjaśnił, że wartością samą w sobie dla przedsiębiorcy przystępującego do certyfikacji jest wzrost poziomu bezpieczeństwa i doskonałości cyfrowej.

Pani Dyrektor Marianna Sidoroff wyjaśniła, że MRiT wraz z NASK zrealizuje przedsięwzięcie bazujące na kwestiach cyberbezpieczeństwa z programu „Firma Bezpieczna Cyfrowo", ale także będące ofertą dla firm podlegających pod CRA oraz objętych KSC. Wskazała, że certyfikacja jest odnogą działań dot. przedsiębiorców na najniższym bazowym poziomie cyberbezpieczeństwa. Realizowana jest także kampania edukacyjno-informacyjna dla przedsiębiorców o technologiach cyfrowych, e-usługach publicznych, podnosząca poziom cyberbezpieczeństwa. Kolejnym działaniem jest program transformacji cyfrowej przedsiębiorstw. Ponadto wspólny program planowany z MC w kontekście doradztwa, które wchodzi do MŚP czy współpraca z NGO'sami i z dużymi firmami technologicznymi – to pakiet działań, które mają przeprowadzić zmiany w funkcjonowaniu MŚP. Pan Dyrektor powiedział, że bardzo istotne jest upowszechnianie wiedzy o normach, standardach, specyfikacjach technicznych wśród małych, średnich, dużych przedsiębiorstw. System oceny zgodności może zapewniać jakość cyberbezpieczeństwa. Warunkiem jest rozwijanie kompleksowo, holistycznie w kierunkach procesów, produktów, usług, systemów zarządzania oraz kompetencji.

Obecny na posiedzeniu Pan Premier Krzysztof Gawkowski wskazał, iż należy jasno powiedzieć, że certyfikacja powinna wpływać na odpowiedzialność biznesową i na odpowiedzialność całego procesu zamówień publicznych, ponieważ wtedy będzie zrozumiały cel jej wykonania. W dalszej części wypowiedzi Pan Premier podziękował członkom Rady za rok pracy, przede wszystkim za pracę wykonaną w kilku obszarach strategicznych dla MC –

Strategii Cyfryzacji Polski oraz ustawie o nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Pan Premier wskazał plany na 2025 rok - zajęcie się bezpieczeństwem dzieci w internecie oraz zamknięcie sprawy legislacyjnej dot. ochrony przed nielegalnymi treściami, szkodliwymi treściami, patostream'em, elementami weryfikacji wieku. Pan Premier poinformował, że od 2025 r. będą wydawane komunikaty, a następnie rekomendacje, które zgodnie z KSC mają charakter obligatoryjny dla całego rynku dot. platform. Pan Premier wskazał, że czas zająć się modyfikacją przepisów dot. cyberprzestępców, ponieważ w skali incydentów cyberprzestępczość ciągle rośnie. W związku z polską prezydencją w Radzie UE istotną i trudną sprawą będzie ochrona dzieci w internecie.

Wdrożenie AI Act – Pani Pamela Krzypkowska, Dyrektor Departamentu Badań i Innowacji w MC.

Pani Dyrektor Pamela Krzypkowska opowiedziała o projekcie ustawy o systemach sztucznej inteligencji odnoszącej się do wdrożenia AI Act oraz o obecnych działaniach związanych z wdrożeniem Aktu o Sztucznej Inteligencji. Obecnie analizowane są uwagi zgłoszone w ramach konsultacji społecznych, które nakreśliły kierunek zmierzania ustawy. Pani Dyrektor jako najistotniejsze wskazała:

- uproszczenie systemu kontroli - zauważono, że opis kontroli był sformułowany zbyt skomplikowanie i proceduralnie;
- ułatwienia dla przedsiębiorców - dla wdrażających i tworzących systemy sztucznej inteligencji;
- prosta komunikacja – planowane jest przeprowadzenie webinaru związanego z systemami *general purpose AI*, aby wytłumaczyć na czym polegają zapisy dla tworzących/wykorzystujących systemy AI;
- sposób zapewnienia stworzenia fabryki AI, która ma za zdanie zbudowanie ekosystemu dookoła sztucznej inteligencji – nie tylko infrastruktura, ale także sieciowanie i budowanie wspólnoty akademicko-biznesowej, także z administracją publiczną.

Pani Dyrektor wskazała, że w odniesieniu do samej ustawy najważniejsze są różne perspektywy co do powołania samego urzędu, własność urzędu oraz skład komisji. Największe uwagi dotyczą składu komisji – jednostki mające głos, uczestniczące w posiedzeniach oraz Rada Społeczna. Poza samą ustawą istotny jest ekosystem także w perspektywie prezydencji. W czasie polskiej prezydencji, do AI Act wejdą dwa kluczowe elementy: systemy zakazane do użycia w całej UE - *scoring społeczny* oraz tzw. *general purpose AI code of practice.* W dalszej części wypowiedzi Pani Dyrektor wspomniała, że głównym wyzwaniem komunikowanym do *AI Office* jest jednolity rynek cyfrowy. Z kolei na pierwsze posiedzenie *AI Board* planowane jest stworzenie wykazu poszczególnych państw członkowskich, ich systemów wdrażania i związanych z tym nadzorem rynku. Ponadto, jednym z innych priorytetów jest wsparcie MC przez NASK w stworzeniu warsztatu podczas

prezydencji związanego ze standaryzacją AI i elementami cyberbezpieczeństwa. Pani Dyrektor wspomniała, że prowadzone będą dyskusje oraz rozmowy z KE na temat działań związanych z fabrykami AI. Priorytetami MC jest współpraca fabryk, możliwość łatwego opisu w jaki sposób MŚP i startupy będą miały dostęp do mocy obliczeniowej oraz tzw. *AI applied strategy* – uaktualnienie polityki AI. KE stworzy *applied strategy*, która dot. sposobu aplikowania/używania sztucznej inteligencji. Podsumowując, Pani Dyrektor poinformowała, że fabryki AI oraz strategia są wspólnym i bardzo ważnym elementem, nad którym MC będzie pracować.

W toku dyskusji zapytano m.in. o piaskownice AI. Pani Dyrektor odpowiedziała, że każde państwo członkowskie musi mieć co najmniej jedną piaskownicę wspólną lub jednego państwa. Obecnie, pod zastanowienie poddano kwestię o posiadaniu jednej lub większej liczby piaskownic sektorowych.

Sprawy różne.

Rozmawiano na temat spotkania członków Rady z Panem Ministrem Dariuszem Standerskim w sprawie eIDAS. Zaproponowano także zastanowienie się nad kwestią definicji treści nielegalnych w kontekście ustawy wdrażającej DSA. Pani Przewodnicząca poinformowała, że pierwsze posiedzenie Rady w styczniu 2025 r. zostanie poświęcone dyskusjom wewnętrznym Rady.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Agnieszka Jankowska – Przewodnicząca
6. Jolanta Jaworska
7. Michał Kanownik
8. Katarzyna Kopczewska
9. Janusz Kosiński
10. Anna Beata Kwiatkowska
11. Jarosław Mojsiejuk
12. Krzysztof Silicki
13. Patrycja Staniszewska
14. Robert Trętowski
15. Sławomir Wojciechowski
16. Małgorzata Zakrzewska

Zaproszeni goście:

17. Krzysztof Gawkowski, Wicepremier, Minister Cyfryzacji
18. Pamela Krzypkowska, Dyrektor Departamentu Badań i Innowacji w MC
19. Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w MC
20. Paweł Kostkiewicz, Dyrektor Ośrodka Standaryzacji i Certyfikacji w NASK
21. Marianna Sidoroff, Dyrektor Departamentu Gospodarki Cyfrowej w Ministerstwie Rozwoju i Technologii

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

22. Karolina Taczalska, Biuro Ministra w MC
23. Joanna Gójska, Biuro Ministra w MC