Warszawa, dnia 26 kwietnia 2017 r.

PROTOKÓŁ

z V posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 21 kwietnia 2017 roku, o godzinie 12:30 w siedzibie Ministerstwa Cyfryzacji.

1. **Informacja liderów zespołów roboczych nt. realizacji projektów oraz postępów prac w zespołach.**

Członkowie Rady do Spraw Cyfryzacji dyskutowali nad podjętymi w ramach poszczególnych zespołów ustaleniami. Przedstawiono następujące informacje:

- Zespół nr I – przegląd prawodawstwa w poszukiwaniu luk i barier procesu cyfryzacji

Utworzona w ramach zespołu ds. przeglądu prawodawstwa w poszukiwaniu luk i barier procesu cyfryzacji ankieta została przekazana do konsultacji w ramach Departamentów Ministerstwa Cyfryzacji tj. Departamentu Prawnego oraz Departamentu Cyberbezpieczeństwa. Jeśli chodzi o kwestie techniczne, ankieta wymaga korekty (wiąże się z poniesieniem kosztów, które muszą zostać zaakceptowane przez MC), co za tym idzie nie została ona jeszcze udostępniona publicznie.

- Zespół nr II - systemowe wsparcie dla cyfrowej transformacji gospodarczej

Lider zespołu ds. systemowego wsparcia dla cyfrowej transformacji gospodarczej spotkał się z Panem Janem Staniłko, Zastępcą Dyrektora Departamentu Innowacji Ministerstwa Rozwoju. Spotkanie związane było z trwającymi pracami nad budową strategii cyfrowej transformacji gospodarki i miało na celu zapoznania się z prowadzonymi przez MR pracami w tym obszarze. Przedstawione zostały również zadania Rady ds. Cyfryzacji i jej poszczególnych zespołów. Ze strony przedstawiciela MR padła propozycja, aby Rada ds. Cyfryzacji wspomogła resort rozwoju w opracowaniu takowej strategii. Rolą Rady nie jest jednak stworzenie samej strategii - Rada mogłaby i stworzy dokument wyjściowy do strategii, tzw. Green Paper – dokument kilkunastostronicowy, wyjściowy do strategii, określający obszary i cele szczegółowe, które należy rozwinąć (coś na kształt niemieckiego Green Paper Labour 4.0.). Członkowie Rady zostali poproszeni o zgłaszanie się do prac nad tym dokumentem, poproszono o sugestie, co do zaproszenia przedstawicieli z różnych branży oraz określenia harmonogramu prac nad przedmiotowym dokumentem.

- Zespół nr III - otwartość danych i oprogramowania finansowanego ze środków publicznych

Zespół ds. otwartości danych i oprogramowania finansowanego ze środków publicznych poinformował, że na ten moment nie posiada jeszcze informacji z MC nt. treści spływających sprawozdań Pełnomocników Otwartości Danych z poszczególnych ministerstw, jak również wyników inwentaryzacji danych w różnych instytucjach publicznych. Z informacji otrzymanych z resortu wynika, że takie dane zostaną przekazane na początku maja br. Po ich otrzymaniu zespół przystąpi do konsultacji i zgłaszania uwag zarówno do inwentaryzacji jak i sprawozdań Pełnomocników. Ponadto zespół jest w kontakcie z KRMC, by Komitet dokonując oceny projektów brał pod uwagę kwestię otwartości danych.

W kwestii oprogramowania i tematyki dalszego udostępniania kodu, zespół przygotował ankietę – prośbę o komentarze z rynku dotyczące:

- Kosztów i korzyści związanych z wykorzystaniem otwartych źródeł w administracji,
- problemów prawnych w przekazaniu praw do źródeł programów, które już są w administracji,
- modeli biznesowych, które są wspierane przez otwarte oprogramowanie oraz tych, którym nie jest po drodze z otwartym oprogramowaniem w administracji,
- korzyści dla polskiej gospodarki związanych z nowym modelem zamawiania oprogramowania przez administrację publiczną.

Ankieta ma zostać adresowana do szerokiej grupy odbiorców. Istotna będzie wsparcie komunikacyjne MC .

- Zespół nr IV - zarządzanie internetem i neutralność sieci

Zespół ds. zarządzania internetem i neutralności sieci przygotował zestaw pytań (ankietę) dedykowany twórcom i odbiorcom treści w internecie, jak również telekomom i organizacjom zajmującym się wolnością przepływu informacji w sieci. Pytania dotyczą neutralności w sieci - czyli równego traktowania każdego rodzaju informacji w internecie, kiedy ta neutralność jest wskazana, a kiedy trzeba myśleć o wyjątkach. Pytania dotyczyć będą jednak także treści niepożądanych - chodzi o uzyskanie informacji, jakie są rekomendowane modele walki z niepożądanymi treściami (w różnych ich kategoriach) oraz jakie są niepożądane skutki uboczne sugerowanych modeli walki z niechcianymi treściami. Po zebraniu pierwszych informacji planowany jest kolejny etap, polegający na indywidualnych rozmowach z ekspertami, którzy mogliby doprecyzować odpowiedzi na pytania zespołu.

- Zespół nr V - edukacja cyfrowa

Zespół ds. edukacji cyfrowej poinformował, że pracował nad dwoma kluczowymi obszarami, związanymi z: 1) tworzeniem wizji rynku pracy oraz 2) tworzeniem założeń programowych dla uczelni wyższych w kontekście listy przedmiotów (z ogólnymi założeniami, co powinno znaleźć

się w programie). Na ten moment ze zgromadzonych informacji zaczyna się rysować podejście metodologiczne dzięki, któremu zbadany może zostać deficyt zawodów. Zespół planuje uruchomienie komunikacji z rynkiem w obszarze badania luk i braków zawodów. Na jesieni ma powstać ankieta internetowa, która pozwoli zebrać informacje, jakich kompetencji brakuje w tym sektorze. Została wykonana metodyczna praca w obszarze zdefiniowania tzw. *body of knowledge* dla informatyki – połączone zostały dwa kluczowe obszary: *computer science* i *computer engineering* z opisem i nazwami przedmiotów oraz ilości godzin.

Zespół prosi o udział na kolejnym posiedzeniu Rady Dyrektora Departamentu Kompetencji Cyfrowych MC, by przedstawił Radzie zagadnienia, jakimi zajmuje się jego departament w obszarze edukacji cyfrowej. Zespół oczekuje również spotkania Zespołu z nowo wybranym Liderem Cyfryzacji, ponieważ obszar związany z *digital skills*, czyli z rozszerzaniem kompetencji cyfrowych jest adresowany dla lidera cyfryzacji.

2. **Zajęcia przez Radę stanowiska w odniesieniu do problemu pt. handel w niedzielę, a sklepy internetowe.**

Członkowie Rady po dyskusji na temat zakazu handlu w niedzielę, w tym w szczególności handlu internetowego, jednogłośnie ustalili, że nie będą się zajmować tym tematem, chyba, że okaże się, że potrzebne jest pilne wsparcie Rady. Nad projektem ustawy trwają od dłuższego czasu intensywne prace w Sejmie, w które zaangażowane są różne środowiska - wypracowywany jest kompromis. Ponadto jest to inicjatywa obywatelska, a Rada działa, jako ciało doradcze dla Ministra Cyfryzacji, co również jest przesłanką by nie podejmować się tego tematu.

3. **Wprowadzenie do tematu nieprawdziwych informacji pojawiających się w internecie. Prezentacja aktualnych przepisów i możliwości zwalczania nieprawdziwych treści. Dyskusja i omówienie planu dalszych działań RdC w tym obszarze.**

Żeby dobrze zrozumieć problem nieprawdziwych informacji (tzw. *fake news*) pojawiających się w internecie, należy przeanalizować zmiany zachodzące w sferze mediów, gdyż są tu społeczno - ekonomiczne przyczyny problemu. Istotne zmiany w obszarze mediów podzielić można na trzy strefy:

- produkcję informacji,
- modele biznesowe, na których producenci informacji i treści zarabiają,
- sposób dystrybucji informacji.

Na istotne zmiany w produkcji informacji składa się kilka czynników - kwestia ilość informacji, która jest produkowana i w obiegu, liczba producentów (każdy użytkownik, firma, organizacja potencjalnie może zostać producentem, twórcą informacji, twórcą mediów). Następuje deprofesjonalizacja zawodu dziennikarza. Kluczowym aspektem obiegu informacji staje się uwaga użytkowników – im więcej „kliknięć", tym większy zarobek przedsiębiorców. Istotnym elementem tego modelu biznesowego i ekonomii uwagi jest to, że koszt produkcji informacji/

publikacji informacji w internecie jest bardzo niski, a co za tym idzie można to robić w zasadzie bez ograniczeń. Jednocześnie zakładając, że każda informacja, która jest opublikowana, jest w stanie przyciągnąć uwagę użytkowników, to nie ma motywacji do „przesiewania" informacji idących do publikacji, ponieważ każda z nich potencjalnie generuje przychody. Jest szereg badań pokazujących tzw. regułę „długiego ogona", co oznacza, że większy przychód generuje duża ilość treści mało popularnych niż niewielka liczba najbardziej popularnych. Co za tym idzie przy tak dużej produkcji informacji mamy do czynienia ze spadkiem ich jakości. Kolejną istotną kwestią jest to, że media internetowe rezygnują z bardzo tradycyjnej roli, którą dotąd pełniły tj. instytucji, która dokonuje weryfikacji najważniejszych i najistotniejszych tematów, ponieważ opłaca się publikować jak najwięcej i jak najszybciej, niekoniecznie dokonując przy tym weryfikacji. Natomiast selekcja tego, co jest udostępniane jest dokonywana nie w redakcjach ani nie przez redaktorów tylko jest dokonywana przez użytkowników poprzez serwisy i portale społecznościowe.

W dalszej części dyskusji omówione zostały zasady odpowiedzialności za rozpowszechnienie nieprawdziwych informacji w internecie. Przedstawiono reguły odpowiedzialności na gruncie przepisów ustawy o zwalczeniu nieuczciwej konkurencji (art. 3, art. 14 uznk) oraz ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym. Wskazano na wątpliwości prawne dotyczące zamieszczania sprostowań wiadomości nieprawdziwych w prasie elektronicznej (prawo prasowe), jak również na zasady odpowiedzialności za naruszenie dóbr osobowych poprzez rozpowszechnienie nieprawdziwych informacji. Przedstawiono prawidła dotyczące wyłączenia odpowiedzialności dostawy usług wynikające z ustawy o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. Zaproponowano kierunki dalszej analizy prawnej i dyskusji.

4. **Prezentacja NCCyber – prezentacja planu działania – Dyrektor Krzysztof Silicki, Pani Zuzanna Polak NASK. Dyskusja o obszarach w jakich możliwa byłaby współpraca poszczególnych zespołów zadaniowych.**

Cyberbezpieczeństwo to temat „gorący" ze względu na wzrost zagrożeń (pod kątem stopnia zaawansowania i ich skali). Mówiąc o cyfryzacji, jednolitym rynku cyfrowym czy uzależnieniu gospodarek i społeczeństwa od technologii teleinformatycznych kwestie cyberbezpieczeństwa są coraz bardziej przybierają na znaczeniu. Poza wykorzystaniem inicjatyw, które funkcjonują od lat (jak CERTy, tj. zespoły zajmujące się reagowaniem na zagrożenia, w tym działający w NASK CERT Polska) pojawiają się regulacje typu dyrektywa NIS, rozporządzenie RODO czy rozporządzenie eIDAS. Widoczne jest strategiczne podejście do uwzględnienia cyberbezpieczeństwa jako elementu składowego powodzenia cyfrowej transformacji. Cyberbezpieczeństwo jest bowiem związane np. z problemem przestępstw natury gospodarczej/ekonomicznej, ale również z kwestiami cyberterroryzmu czy cyberszpiegostwa. Są to więc obszary kluczowe dla bezpieczeństwa państwa, co wymaga całościowego podejścia do tej tematyki. Z tego względu trwają w MC prace nad dokumentem pt. Strategia

Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022. W skład międzyresortowej grupy pracującej nad dokumentem wchodzili przedstawiciele różnych instytucji (ministerstw Cyfryzacji, Obrony Narodowej, Spraw Wewnętrznych i Administracji oraz Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa, Biura Bezpieczeństwa Narodowego oraz NASK) po to, by uwzględnić tematykę z różnych punktów widzenia. Następnym krokiem ma być ustawa o krajowym systemie cyberbezpieczeństwa - transpozycja dyrektywy NIS. Mowa jest tu więc o aspektach ochrony tzw. kluczowych zasobów i usług z punktu widzenia gospodarek poszczególnych krajów. Ale dyrektywa przewiduje też mechanizmy do współpracy na szczeblu europejskim – zarówno na poziomie operacyjnym (sieć CERTów), jak i na poziomie strategicznym, w grupie współpracy przedstawicieli rządów poszczególnych krajów, którzy wspólnie starają się wypracować najlepsze metody istotnego zwiększenia poziomu cyberbezpieczeństwa w UE (mając na uwadze potrzebę dopasowania się do kluczowych strategii takich jak Jednolity Rynek Cyfrowy).

W lipcu 2016r. powstała inicjatywa powołania NCCyber, czyli Narodowego Centrum Cyberbezpieczeństwa, które powstało w NASK. 4 lipca ubiegłego roku zostało zawarte porozumienie trójstronne między Ministerstwem Cyfryzacji, NASK i Związkiem Banków Polskich o współpracy w zakresie budowy systemu partnerskiego dla cyberbezpieczeństwa w Polsce. NCCyber zostało zbudowane w oparciu o istniejące zasoby (np. zespół CERT Polska, dyżurnet.pl). Obecnie NCCyber składa się z czterech filarów:

1. Dział NSOC => jest to zespół operacyjny, zajmujący się przyjmowaniem zgłoszeń, bieżącą oceną stanu cyberbezpieczeństwa i współpracą z partnerami. Działa 24h/dobę i jest pierwszą linią, do której trafiają wszelkie informacje o incydentach (i tych technologicznych i tych dotyczących nielegalnych i szkodliwych treści). Tu jest dokonywana wstępna analiza sytuacji i tu powstają raporty dobowe przesyłane do MC i do RCB.
2. Dział CERT Polska => zespół analityczny, który zajmuje się najpoważniejszymi incydentami i dokonuje zaawansowanych analiz technologicznych. Jest to hub wymiany informacji – współpracuje z innymi CERTami w kraju i za granicą. Jest to serce i mózg NCCyber - miejsce, w którym zbierana jest zaawansowana wiedza technologiczna i doświadczenie w dziedzinie cyberbezpieczeństwa.
3. Dział Rozwoju, Polityk i Standardów => zespół ten zajmuje się wypracowaniem pewnych standardów, polityk i dobrych praktyk związanych z kwestiami cyberbezpieczeństwa. Tu budowane jest zaplecze dla tworzenia analiz i rekomendacji, a także audytów zgodności z pewnymi wytycznymi.
4. Dział Współpracy, Komunikacji i Szkoleń => tu nacisk kładziony jest na szkolenia, studia podyplomowe itp. Istotna jest np. potrzeba szkoleń dla organów ścigania, bo pojawiają się nowe przestępstwa określonej natury – ich poznanie nieraz wymaga pozyskania wiedzy choćby z CERTów właśnie. Również ćwiczenia w cyberbezpieczeństwie są istotne, by pracować na konkretnych scenariuszach zagrożenia, by wiedzieć co się nie sprawdza w sytuacjach kryzysowych, co nie działa i co można poprawić.

Istotne jest zaangażowanie do inicjatywy NCCyber partnerów kluczowych, którzy chcą dzielić się swoją wiedzą. Na ten moment z NCCyber współpracuje ok 50 partnerów. NASK zachęca do współdziałania kolejnych przedstawicieli różnych sektorów – bankowości, energetyki, transportu i wszelkich sektorów krytycznych.

Kluczowa dla bezpieczeństwa cybernetycznego jest również kwestia współpracy pomiędzy CERTami – obok CERT Polska, jest jeszcze CERT.GOV.PL i CERT-MIL oraz mniejsze CERTy. Chodzi o to, by wszystkich zaangażować, nikogo nie pominąć i nie wykluczyć. Współpraca operacyjna i wymiana informacji o zagrożeniach możliwa będzie na platformie współpracy analitycznej – będzie to miejsce, w którym można dzielić się technologiczną informacją dotycząca incydentów naruszenia bezpieczeństwa (Co to za incydent? Jaka była jego natura? Jakie były wektory ataku? Jakie wskaźniki są z nim związane?), by przez dogłębne analizy można było ostrzegać innych.

W grudniu ubiegłego roku Ministerstwo Cyfryzacji powołało Forum Cyberbezpieczeństwa. Ma to być projekt szerokiego partnerstwa publiczno-prywatnego w obszarze cyberbezpieczeństwa. Jedną z grup w ramach Forum jest grupa powołana do spraw rozwoju NCCyber. Zebranie w grupie strategicznych partnerów pozwoli z jednej strony uzyskać wiedzę na temat oczekiwań wobec działalności Centrum. Z drugiej zaś strony będzie to możliwość zaproponowania pewnych sposobów wymiany informacji i podjęcia wspólnej pracy. NCCyber stawia bowiem bardzo mocno na współpracę.

Możliwa jest także współpraca z Radą do Spraw Cyfryzacji:

a) Jednym z zadań zespołów roboczych Rady jest przegląd prawodawstwa przy poszukiwaniu luk i barier w zakresie transformacji cyfrowej i budowania systemu cyberbezpieczeństwa. Szukanie ograniczeń prawodawstwa odbywać się może wspólne – np. grupa zajmująca się rozwojem NCCyber w ramach Forum Cyberbezpieczeństwa może pomóc Radzie wypracować pewne rozwiązania legislacyjne, lub wskazać te problemy regulacyjne, które w ramach bieżącej współpracy operacyjnej się pojawiają. Działania Rady w zakresie poszukiwania luk i barier muszą być spójne z działaniami MC i jednostek podległych, stąd również bieżący kontakt z Departamentem Cyberbezpieczeństwa. Istotne jest by nie powielać działań i rozszerzyć planowaną przez Radę ankietę o kwestie związane z cyberbezpieczeństwem. Zapis o potrzebie przeglądu prawodawstwa a tym zakresie wynika również z zapisów Strategii Cyberbezpieczeństwa RP.
b) NASK mógłby również pomóc Radzie odpowiedzieć na pytanie dotyczące bezpieczeństwa otwartego oprogramowania i dostępu do kodów źródłowych – przygotowanie rekomendacji dotyczących oprogramowania zamawianego przez administrację publiczną w kontekście otwartości tego oprogramowania jest jednym z zadań Rady. Nie da się jednak uniknąć w tym temacie pytania o bezpieczeństwo takich rozwiązań.

c) Rada została również zaproszona do współpracy przy stworzeniu ogólnych wytycznych do szczegółowej strategii transformacji cyfrowej dla Ministerstwa Rozwoju. Z punktu widzenia całości rozwoju gospodarki cyfrowej komponent bezpieczeństwa jest kluczowy, choćby pod kątem rozwiązań IoT w ramach infrastruktury krytycznej. Tu też współpraca z NASK byłaby cenna.

5. Spotkanie z Panią Dyrektor Wandą Buk Centrum Projektów Polska Cyfrowa dotyczące aktualnego stanu wykorzystania środków unijnych w ramach II osi PO PC

Spotkanie z przedstawicielami Centrum Projektów Polska Cyfrowa (w celu m.in. uzyskania wiedzy na temat aktualnego stanu wykorzystania środków unijnych w ramach PO PC) zarekomendował Radzie Minister Piotr Woźny, podczas spotkania z Radą na posiedzeniu w lutym br.

Rada jest zainteresowana możliowością konsultowania kryteriów, według których wybierane są projekty do realizacji, mając na uwadze cel nadrzędny, jakim jest transformacja cyfrowa polskiej gospodarki.

Program Operacyjny Polska Cyfrowa (PO PC) jest jednym z 6 krajowych programów operacyjnych na lata 2014-2020. Jest to 10 mld zł nie tylko na budowę e-administracji (II oś), ale i na internet szerokopasmowy (I oś) oraz rozwój cyfrowych kompetencji społeczeństwa (III oś). Alokacja środków w ramach I i II osi jest podobna i wynosi (w przeliczeniu kwot w Euro) po ok. 3,5 – 4 mld. zł.

Przedmiotem dyskusji jest przede wszystkim II oś - celem wsparcia jest tu poszerzenie zakresu spraw, które obywatele i przedsiębiorcy mogą załatwić drogą elektroniczną. Bezpośrednio będzie się to odbywać poprzez elektronizację nowych usług publicznych oraz poprawę funkcjonalności i e-dojrzałości usług istniejących. Pośrednio natomiast – poprzez usprawnianie usług wewnątrzadministracyjnych (A2A), niezbędnych dla świadczenia usług publicznych. Ponadto wsparcie będzie ukierunkowane na poprawę pracy urzędów poprzez cyfryzację procesów i procedur, jak również na udostępnienie informacji sektora publicznego, takich jak dane pochodzące ze źródeł administracyjnych, zasoby kultury oraz zasoby nauki.

Na II oś PO PC składają się:

1. Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”
2. Działanie 2.2 „Cyfryzacja procesów back-office w administracji rządowej”
3. Działanie 2.3 „Cyfrowa dostępność i użyteczność informacji sektora publicznego”
4. Działanie 2.4 „Tworzenie usług i aplikacji wykorzystujących e-usługi publiczne i informacje sektora publicznego”

Największa alokacja środków dotyczy działania 2.1 – odbyły się dotychczas cztery nabory (przy czym nabór trzeci został anulowany). W następstwie naboru pierwszego i drugiego w realizacji jest 17 projektów (łączna alokacja środków na nie wynosi 1,5 mld zł – jest więc to praktycznie

połowa kwoty, przeznaczonej na działanie 2.1). Umowy w zakresie projektów z tych dwóch naborów podpisywane były do końca pierwszego kwartału ubiegłego roku. Po półtora roku niecałe 3% środków zostało wydanych (33 mln zł). Jest to dramatyczna informacja dla instytucji pośredniczącej, jaką jest CPPC, gdyż Polska, jako państwo członkowskie UE, ma zobowiązania nałożone przez Komisję Europejską. Obowiązuje nas zasada N+3, którą musimy spełnić – co uda się, ale jedynie dzięki osi I, gdzie np. tylko w ostatnim kwartale ubiegłego roku wydane, bez instrumentów finansowych, zostało 100 mln zł (czyli trzy razy więcej, niż przez półtora roku w osi II). Postępowania kuleją choćby przez braki kadrowe w administracji publicznej, w której nie ma odpowiedniego nasycenia specjalistami zajmującymi się projektami informatycznymi, gdyż rynek oferuje im dużo większe wynagrodzenia - praca w administracji nie jest dla nich atrakcyjna. Każde postępowanie można również przedłużać poprzez składanie licznych pytań, wniosków, skarg do sądu. Również restrykcyjne zapisy (i konieczność ich przestrzegania) Prawa Zamówień Publicznych odbijają się na procedowaniu projektów.

Projekty w pierwszym i drugim konkursie zostały wybrane na podstawie bardzo szerokich kryteriów. Nie były one weryfikowane pod kątem powielania się, wpisywania się w strategię informatyzacji itp. Pokłosiem tego było anulowanie trzeciego konkursu. Przemodelowane zostały kryteria naboru – pracował nad nimi zespół ekspertów, jednak na pewno są rzeczy, które można jeszcze poprawić. Dodatkowo (czego nie było w pierwszym i drugim naborze) nie ma takiej możliwości, żeby dofinansowanie dostał projekt, który nie został pozytywnie zaopiniowany przez Komitet Rady Ministrów do spraw Cyfryzacji (KRMC). Najpierw jest więc preweryfikacja na poziomie KRMC – pozwala to jeszcze na wprowadzenie zmian do projektu, udoskonalenie go, wpasowanie w architekturę. Zwiększa to szansę na dostanie dofinansowania. Bo w chwili, gdy wniosek trafia już do CPPC nie ma możliwości modyfikowania go – CPPC jako instytucja organizująca konkurs działa w sztywnych ramach określonych przez KPA i jeśli wniosek trafi więc już do Centrum można go jedynie ocenić pozytywnie, lub negatywnie. Na etapie oceny wniosek nie może być już więc poprawiany, nie można wprowadzać już w nim żadnych zmian.

Ze względu na etap weryfikacji przez KRMC i fakt, że Komitet nie przepuścił wielu projektów, z alokacji na 600 mln zł obecnie wartość projektów w ostatnim konkursie wynosi ok 300 mln zł – takie będzie więc wykorzystanie środków zakładając, że wszystkie wnioski przejdą pozytywie etap oceny. Z tego względu planowane jest ogłoszenie kolejnego naboru (oraz ewentualne dalsze ponawianie konkursów w miarę potrzeb). Wzięcie pod uwagę eksperckiej opinii Rady na temat kryteriów w kolejnych konkursach jest więc jak najbardziej możliwe – CPPC wykazuje również wolę do konsultowania z Radą tych kwestii.

Co jednak również istotne Komisja Europejska pozwoliła na wykorzystanie w II osi nie tylko trybu konkursowego (jak było dotychczas), ale również trybu indykatywnego – oznacza to brak konieczności przeprowadzania konkursów na strategiczne projekty z punktu widzenia państwa. Beneficjentem tych projektów będzie Minister Cyfryzacji. Jest to pewne światło w

tunelu, pozwala mieć nadzieję, że środki na tej osi nie przepadną. Trzeba mieć bowiem świadomość, że jest to ostatnia perspektywa finansowa i że nie ma już możliwości fazowania projektów, jak to miało miejsce dotychczas.

Podczas spotkania zwrócono jeszcze uwagę na działania III osi PO PC, nakierowanej na cyfrowe kompetencje społeczeństwa. Interwencja w osi III adresowana będzie do grup o zróżnicowanych poziomach kompetencji cyfrowych, ze szczególnym uwzględnieniem działań na rzecz włączenia cyfrowego (np. naukę podstawowych kompetencji cyfrowych do osób 65+). Planowany jest również np. konkurs na naukę korzystania z e-usług, jednak te trzeba najpierw wytworzyć właśnie w osi II.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht – Przewodnicząca
2. Michał Adamczyk

3. Dominik Batorski
4. Roman Bieda
5. Karol Dobrzeniecki
6. Alicja Grawon-Jaksik
7. Krzysztof Goczyła
8. Łukasz Jachowicz
9. Dariusz Milka
10. Tomasz Muda
11. Jerzy Nawrocki
12. Rafał Rodziewicz
13. Justyna Skorupska
14. Maciej Sobolewski
15. Piotr Waglowski
16. Janusz Zawiła - Niedźwiecki

Zaproszeni goście:

17. Krzysztof Silicki NASK
18. Zuzanna Polak NASK
19. Wanda Buk CPPC

Sekretariat Rady:

20. Justyna Grzegorek (MC)
21. Katarzyna Stopińska (MC)