

UCHWAŁA nr 4
RADY do SPRAW CYFRYZACJI
z dnia 20 maja 2022 roku
w sprawie Cyfrowego Narodowego Zasobu Informacyjnego.

Na podstawie art. 17 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 17 Ministra Cyfryzacji z dnia 24 czerwca 2020 r. w sprawie ustanowienia regulaminu Rady do Spraw Cyfryzacji (Dz. Urz. z 2020 r. poz. 19), uchwała się, co następuje:

Polityka otwartości zasobów od kilku lat jest stałym elementem dyskusji na forum Unii Europejskiej. Analizując kwestię otwartości zasobów należy przede wszystkim zwrócić uwagę na nieprecyzyjność i brak definicji terminów „zasoby cyfrowe”. Pojęcie to obejmuje także dane nie mieszczące się w definicji informacji publicznej, czy informacji sektora publicznego, o której mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego¹ (dyrektywa w sprawie otwartych danych) i dotyczy także tych zasobów, które stanowią przedmiot proponowanych regulacji w projektach rozporządzeń Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi.

Pierwotnie inicjatywa otwartości zasobów cyfrowych wiązała się z bezpłatnym dostępem do zasobów finansowanych ze środków publicznych, co zdaje się obejmowało również informacje, których udostępnianie nie leżało w gestii podmiotów publicznych. Na ten ostatni element wskazywali zwolennicy otwartości zasobów wyrażając stanowisko, iż „ograniczenia dostępu wynikające z praw autorskich (lub innych zasad dotyczących sposobu korzystania z treści)” są „sprzeczne z polityką dostępności zasobów publicznych”, przez co „należy ich unikać lub traktować jako wyjątek od reguły”.

Obecnie w projektowanych rozporządzeniach UE już nie ma wątpliwości, iż chodzi o dane będące w posiadaniu organów sektora publicznego i prywatnego, które są objęte prawami innych osób, a zatem wykraczają poza zakres wspomnianej dyrektywy re use.

Tego rodzaju ujęcie problematyki otwartości zasobów cyfrowych jest trudne w realizacji nie tylko z powodu wiążących Polskę standardów międzynarodowych dotyczących ochrony praw własności intelektualnej, ale także regulacji wewnętrznych odnoszących się do takich kwestii jak: prawo do prywatności i autonomii informacyjnej (tu także prawo konstytucyjne do bycia informowanym o sposobie przetwarzania danych przez władzę publiczną), prawo własności do posiadanych lub generowanych treści przez jednostkę, tajemnica

¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE OJ L 172, 26.6.2019, p. 56–83)

przedsiębiorcy, ochrona własności przemysłowej, inne tajemnice prawnie chronione, etc. Wątpliwości odnoszą się zarówno do sytuacji prawnej jednostek, jak i przedsiębiorców.

Propozycje zawarte w projektach rozporządzeń UE wydają się interesujące w szczególności dla sektora prywatnego, ponieważ proponowany model tworzy warunki do powstania zaufania co do ochrony danych w przyszłości, w wyniku ich ponownego wykorzystywania. Utrata kontroli nad zasobami, zwłaszcza informacyjnymi, to podstawowe zagrożenie dla bezpieczeństwa personalnego, jak i obrotu handlowego, zwłaszcza w sferze cyfrowej.

Obok powszechnie uznanego przekonania o pozytywnym wpływie, jaki te nowe zobowiązania mogą wywierać na naukę, innowacyjność i przemysły kreatywne, pojawia się problem rozliczeń z tytułu korzystania z własności osób trzecich. Zapewnienie ochrony i wynagrodzenia za podejmowany wysiłek twórczy i intelektualny uprawnionych jest oczywistym standardem. Nowe rozwiązania odnoszą się do wszelkich zasobów prywatnych, będących w posiadaniu sektora publicznego – przy czym to posiadanie może mieć różne źródło (np. może być związane z archiwizacją, ale też z realizacją zadań publicznych przez sektor prywatny).

W konsekwencji nie chodzi tu więc o negowanie konieczności ponownego korzystania z tych danych, czy ochrony praw do tych danych, ale o stosowaną przez organy administracji publicznej strategię w zakresie ustalania warunków i reguł dostępu do treści cyfrowych, których te organy są właścicielami albo prawnymi dysponentami. Należy podkreślić, iż wyjątki i ograniczenia praw autorskich, w tym zasady *fair use* i *fair dealing* zapewniają skuteczną równowagę pomiędzy ochroną twórcy w zakresie jego twórczości wynikającą z praw autorskich lub pokrewnych, a interesem publicznym. Takie mechanizmy gwarantują pewne przywileje, a to z kolei w obecnym systemie prawa własności intelektualnej tworzy wolną przestrzeń do działania. Jednak wobec gwałtownych zmian, tak w sferze technologii, jak i w towarzyszących im zachowaniach społecznych, niezwykle ważne jest zapewnienie możliwości działania z wykorzystaniem narodowych zasobów cyfrowych. Wszelkie ograniczenia praw własności, w tym wspomniane zasady *fair use* i *fair dealing*, powinny być elastyczne i nieustannie dostosowywane do potrzeb i celów interesu publicznego, definiowanego przede wszystkim na poziomie krajowym. Istotne jest tu stanowisko, iż w żadnym wypadku inicjatywy otwierania cyfrowych zasobów publicznych nie powinny zmierzać do pozbawienia lub ograniczenia uprawnień właścicieli praw niebędących podmiotami publicznymi, a wręcz przewidywać zabezpieczenia przed sytuacjami utraty kontroli publicznej nad danymi przekazanymi jednak w zaufaniu do władzy publicznej. W innym przypadku będziemy mieć do czynienia z utratą pewności prawa, niesprawiedliwością społeczną i naruszeniem zasad współżycia społecznego.

Celem nowych regulacji w obszarze otwartości zasobów cyfrowych, stanowiących inicjatywę krajową, jest w głównej mierze usprawnienie ponownego wykorzystywania informacji sektora publicznego w Polsce oraz przyspieszenia procesu otwierania zasobów publicznych. W myśl zasady „as open as possible as closed as necessary” przewidziano podstawę prawną do dobrowolnego udostępniania, za pośrednictwem portalu dane.gov.pl (pełniącego funkcję

centralnego repozytorium informacji publicznej), zasobów informacji będących w posiadaniu także podmiotów sektora prywatnego (np. przedsiębiorców, organizacji pozarządowych).

Pojawia się tu pytanie czy wszystkie zasoby powstałe ze środków publicznych powinny podlegać regule re use? Czy treści te – głównie cyfrowe - podlegają zabezpieczeniom przed nieuprawnionym, nielegalnym korzystaniem w kolejnych etapach, także w warunkach przekazywania danych do państw trzecich. Czy istnieje możliwość odmowy przekazania informacji sektorowi publicznemu w celu re use, w sytuacji, kiedy właściciel danych nie będzie zainteresowany ich dalszym wykorzystywaniem, lub w sytuacji szczególnych zagrożeń dotyczących ponownego wykorzystywania w nieuregulowanej wspólnymi ramami prawnymi cyberprzestrzeni.

Jednym z kluczowych pojęć, którego znaczenie wzrasta wraz z procesami cyfrowymi jest „treść cyfrowa”. Obecnie treści cyfrowe są nierozłącznym i znaczącym elementem codziennych interakcji, jakich dokonują użytkownicy sieci także w sferze publicznej. Treści cyfrowe są to dane, na podstawie których za pomocą odpowiedniego oprogramowania i sprzętu, można po przetworzeniu uzyskać informację, wygenerować nowe dane. Rozpowszechnianie w sieci treści cyfrowych jest z definicji transgraniczne. Korzystają na tym ich producenci, twórcy, ich spadkobiercy, przede wszystkim korzysta odbiorca – użytkownik – beneficjent usługi. Procesy cyfryzacji oraz udostępnianie treści cyfrowych w sposób globalny przyczyniają się do zwiększenia dostępu do wiarygodnych źródeł wiedzy, zasobów pozostających dotychczas w zapomnieniu, nie wyłączając tych pozostających w domenie publicznej, jak i zasobów nowych, także tych powstałych w oparciu o zasoby archiwalne. Kiedy mówimy o treściach cyfrowych w sposób naturalny pojawia się myśl o potrzebie ich ochrony, konieczności zabezpieczenia ich własności w sieci, zwłaszcza kiedy stanowią one dobro prywatne, ale także i tzw. dobro wspólne. Ochrona ta kryje w sobie niezwykle ważny aspekt związany nie tylko z cechami samej twórczości w bardzo wielu dziedzinach ludzkiej aktywności, ale także ze ściśle określoną korzyścią materialną oraz moralną przynależną uprawnionym podmiotom z tytułu własności. Trzeba przy tym pamiętać, iż ochrona własności intelektualnej zachowuje przede wszystkim cel ekonomiczny, ponieważ własność intelektualna jest ściśle związana z procesami tworzenia, rozwijania i wykorzystywania zdobytej wiedzy, a także stanowi wynik ludzkiej twórczości i kreatywności oraz wszelkich inwencji, które stanowią przedmiot obrotu gospodarczego. Zatem, z jednej strony mamy treści cyfrowe – w tym te wypełniające zasoby informacyjne Państwa, z drugiej strony rynek usług związanych z dystrybucją i wszelkim innym korzystaniem z treści cyfrowych, gdzie szczególne znaczenie ma ochrona własności intelektualnej z jej majątkowym i niematerialnym charakterem. Wskazana tu konstrukcja wydaje się oczywista, jeśli chodzi o regulacje dotyczące treści cyfrowych o określonym charakterze, stanowiących utworów. Jednak zaznaczyć trzeba, iż wiele danych nie musi stanowić utworu, a też ich wartość wymaga istotnego zaliczenia ich do zasobu informacyjnego, wymagającego konstytucyjnej ochrony, wynikającej z prawa do własności.

Kultura i nauka pełnią szczególną rolę w życiu społecznym, ze względu na kształtowanie wartościowych postaw jednostki. W związku z czym odpowiedzialność ta w głównej mierze spoczywa na Państwie i to zarówno, jako podmiocie zarządzającym zasobem informacyjnym, będącym dobrem wspólnym narodu, jak też ze względu na kształtowanie postaw obywatelskich oraz uwrażliwianie na konkretne wartości. Rozwój nowych organizacji tworzenia, upowszechniania i ochrony zasobów informacyjnych powoduje, że zakres odpowiedzialności za warunki re use zarówno w aspekcie podmiotowym, jak i przedmiotowym jest wciąż niedookreślony. Można powiedzieć, że proponowane regulacje mogą przyczynić się do fragmentaryzacji odpowiedzialności za cyfrowe zasoby narodowe. Funkcje kontrolne Państwa, bez ich konkretyzacji mogą budzić obawy o zbyt daleko idącą ingerencję.

Korzystanie z informacji sektora publicznego wymaga odpowiedniego zarządzania istniejącymi zasobami informacyjnymi Państwa, polegającego na integracji systemów teleinformatycznych, w ramach całej administracji publicznej, pozwalającego na rozwój społeczny w oparciu o odpowiednie reguły prawne, uwzględniające przesłanki dopuszczalnej ingerencji w prawa i wolności jednostki, zważywszy na charakter danych i świadczonych usług - określonych przede wszystkim na poziomie krajowym. Przepisom prawa towarzyszącym otwieraniu danych powinny towarzyszyć krajowe przepisy określające ich udostępnianie przez podmioty publiczne w sposób:

- 1) przejrzysty i oparty o obiektywne kryteria dla realizacji celów publicznych, w tym także dotyczących społeczności lokalnych;
- 2) uwzględniające różne rodzaje danych i informacji w nich zawartych, np. branżowe czy dane z systemów służących do zarządzania miastami/gminami, w takich obszarach jak: transport (tzw. systemy ITS), bezpieczeństwo publiczne, zarządzanie infrastrukturą, ochrona środowiska czy jakość życia mieszkańców;
- 3) treści, które powinny podlegać tylko ograniczonemu upublicznieniu lub wykorzystaniu ze względu na wartości prawem chronione.

Należy podkreślić, iż otwarcie zasobów publicznych, reguła re use i nowa polityka zarządzania danymi, także tymi prywatnymi, wymaga zharmonizowanych działań o charakterze strategicznym a następnie legislacyjnym oraz współpracy pomiędzy poszczególnymi podmiotami na różnych poziomach budowania cyfrowego, narodowego zasobu informacyjnego.

Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone na posiedzeniu Rady do Spraw Cyfryzacji. Projekt Uchwały nr 4 został poddany głosowaniu w dniu 20 maja 2022 r. W głosowaniu wzięło udział 12 członków Rady z czego oddano:

- 12 głosów „za” przyjęciem uchwały,
- 0 głosów „przeciw” oraz
- 0 głosów „wstrzymuję się”.

Uchwała nr 4 Rady do Spraw Cyfryzacji została przyjęta 20 maja 2022 roku w głosowaniu jawnym zwykłą większością głosów.

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Izabela	Albrycht	za
2.	Andrzej	Dulka	za
3.	Agnieszka	Gryszczyńska	za
4.	Michał	Kanownik	za
5.	Janusz	Kosiński	za
6.	Karol	Krawczyk	za
7.	Mirostaw	Maj	za
8.	Dariusz	Milka	za
9.	Aleksandra	Musielak	za
10.	Józef	Orzeł	za
11.	Paweł	Śniatała	za
12.	Mateusz	Tykiemko	za

Przewodniczący Rady

Józef Orzeł

/-podpisano elektronicznie/